SECRETARIADO DE PUBLICACIONES
UNIVERSIDAD DE SEVILLA

ISBN 84-472-0493-6

La protección del derecho a la libertad informática en la UNIÓN EUROPEA

ÁLVARO A. SÁNCHEZ BRAVO

La protección del derecho a la libertad informática en la UNIÓN EUROPEA

UNIVERSIDAD DE SEVILLA

LA PROTECCIÓN DEL DERECHO A LA LIBERTAD INFORMÁTICA EN LA UNIÓN EUROPEA

LA PROTECCIÓN DEL DERECHO A LA LIBERTAD INFORMÁTICA EN LA UNIÓN EUROPEA

ÁLVARO A. SÁNCHEZ BRAVO

UNIVERSIDAD DE SEVILLA
SECRETARIADO DE PUBLICACIONES
1998

Serie: Derecho
Núm.: 75

© UNIVERSIDAD DE SEVILLA
SECRETARIADO DE PUBLICACIONES. 1998.
C / Porvenir, nº 27. 41013 Sevilla.
Telfs: (95) 423 19 58 - 23 59 76 - Fax: (95) 423 22 45
E-Mail: secpub2@usrec.us.es
© ALVARO A. SÁNCHEZ BRAVO. 1998

Printend in Spain - Impreso en España
I.S.B.N.: 84-472-0493-6
Depósito Legal: S. 1357-1998
Imprime: EUROPA ARTES GRÁFICAS, S.A.

ÍNDICE

A Elisa

PRESENTACIÓN

La Colección *Derecho y Sociedad Tecnológica* se propone dar a conocer investigaciones sensibles al impacto jurídico de las nuevas trayectorias tecnológicas del presente. A ello se dirige la obra del Dr. Alvaro Sánchez Bravo, Profesor Asociado del Departamento de Filosofía del Derecho, Moral y Política de la Universidad de Sevilla, a la que estas breves líneas sirven de pórtico. Se trata de la edición, revisada y actualizada, de la tesis doctoral que tuve la satisfacción de dirigir y que obtuvo la máxima calificación otorgada por un Tribunal presidido por el profesor Dr. Juan-Antonio Carrillo Salcedo e integrado por los profesores: Javier de Lucas, Pablo Lucas Murillo de la Cueva, Carlos Pérez Ruiz y Rafael González-Tablas.

No he de ensayar la supérflua tarea de resumir el libro, cuyos aspectos básicos son certeramente glosados en el *Prólogo* del profesor González-Tablas. Sí me parece, en cambio, oportuno recordar que en las últimas décadas el universo conceptual y contextual de los juristas se ha visto profunda y radicalmente modificado por la transformación de los presupuestos culturales, políticos y económicos que se ha producido en las sociedades tecnológicas del presente. La revolución tecnológica ha redimensionado las relaciones del hombre con los demás hombres, las relaciones entre el hombre y la naturaleza, así como las relaciones del ser humano con su contexto o marco de convivencia. En el curso de estos últimos años pocas cuestiones han suscitado tan amplia y heterogénea inquietud como la que se refiere a las relaciones del hombre con las nuevas nuevas tecnologías. Importa recordar que nos hallamos en una sociedad donde la informática ha devenido el símbolo emblemático de nuestra cultura, hasta el punto de que para designar el marco de nuestra convivencia se alude reiteradamente a expresiones tales como la "sociedad de la información", o a la "sociedad informatizada". La coyuntura presente reclama, por tanto, de los juristas, los filósofos y los teóricos del Derecho una "consciencia tecnologica" ; es decir, una actitud reflexiva crítica y responsable ante los nuevos problemas que, en las diversas esferas del acontecer social suscita la tecnología, y ante los que ni el Derecho, ni quienes lo aplican o lo estudian pueden permanecer insensibles.

Obra lineal, sin disgresiones ni desbordamientos, la del Dr. Sánchez Bravo se dirige, precisamente, al análisis del marco jurídico que, desde la teoría de las libertades, permite adentrarse en un territorio cuya exploración y conquista resultan hoy de actualidad perentoria para los juristas y los ciudadanos más comprometidos con la defensa del Estado de Derecho.

Hoy en España se advierte una voluntad de acercamiento más efectivo a las nuevas tecnologías en la diversidad de sus implicaciones. Han pasado, o están en trance de hacerlo, aquellas aproximaciones trivializadoras -con razón denunciadas por el Dr. Sánchez Bravo- que abordaban los problemas informático-jurídicos sin la requerida erudición teórica y/o sin el sentido crítico necesario para asumir o revisar las fuentes bibliográficas en la materia. Este libro se edifica, por contra, sobre la base indiscutible de un amplio aparato crítico-bibliográfico, que ha sido debidamente analizado y justipreciado. Se trata, en definitiva, de una obra que conjuga la síntesis de amplias lecturas con una concepción personal que brota de la reflexión sobre ellas. Ambos extremos ha logrado el autor con singular acierto y, de este modo, se ha hecho acreedor del reconocimiento de cuantos nos hallamos interesados en el estudio de la disciplina jurídica de la informática.

Antonio-Enrique Pérez Luño
Universidad de Sevilla, octubre de 1997.

PRÓLOGO

Los llamados por la doctrina (Pérez Luño) derechos humanos de tercera generación constituyen la nueva frontera de las *reivindicaciones utópicas* en esta materia, en los mundos donde la sociedad civil ha alcanzado el suficiente grado de desarrollo y estabilidad democrática como para que las libertades públicas (1ª generación) y los derechos económicos y sociales (2ª generación) no sean ya un motivo de especial preocupación. El grado de generalidad y de extensión de los mismos, en el marco del Estado social de derecho, solamente se ve empañado por algunas y puntuales transgresiones de estos derechos que permanentemente nos recuerda la necesidad de mantener una estrecha vigilancia tanto en su protección jurídica como en su constante actualización doctrinal.

El cambiante mundo de hoy, sobre todo en el llamado primer mundo, impone nuevos retos al derecho que tiene que dar una respuesta adecuada a tantas transformaciones. Las novedosas formas de actuación humana abre la puerta a renovados modos de atentar contra los derechos humanos. Transgresiones que hace unos años eran materialmente imposibles de realizar hoy son moneda corriente gracias a la moderna tecnología. La contribución que proporcionan al bienestar humano la genética, las telecomunicaciones o la informática, por solo citar estas, son lo suficientemente evidentes para todo el mundo como para permitirnos eludir su enumeración; pero al mismo tiempo, son una fuente de constantes peligros para los derechos humanos que de ningún modo podemos ignorar.

La necesidad de realizar investigaciones rigurosas que delimiten adecuadamente el uso de todos estos nuevos instrumentos —en el marco de los presupuestos de libertad, igualdad, respeto a la dignidad humana, tolerancia, etc. que han sido los que han permitido la mayor y más práctica realización de la convivencia humana que hasta ahora se conoce en la historia de la humanidad— es una obligación que no debemos omitir los que nos dedicamos al cultivo de la Filosofía del Derecho.

Pues bien, el libro que tengo el placer y el honor de prologar es precisamente uno de estos estudios serios, que analiza en profundidad el nuevo *derecho a la autodeterminación informativa o libertad informática* en el marco donde de una manera más nítida se le está viendo nacer: la Unión Europea. Es también, el paciente trabajo realizado durante años por el Profesor Don Alvaro Sánchez Bravo bajo la siempre sabia dirección de nuestro común *Maestro* Don Antonio-Enrique Pérez Luño, y que fue brillantemente defendida como *Tesis Doctoral* en mayo de 1996, mereciendo a juicio del Tribunal calificador la máxima calificación que permite la ley: «*Apto Cum Laude por unanimidad*». Este hecho, confiere al trabajo, una garan-

tía reforzada de rigor y profundidad en el tratamiento del tema, sin que ello signifique que es de lectura difícil, ya que el Profesor Sánchez Bravo ha sabido dotarle de una prosa ágil y clara que hace muy amena su lectura incluso para los no especialistas. Es pues, una obra que recoge y sistematiza con notable originalidad las aportaciones de los autores más autorizados en la materia, contribuyendo así a llenar un hueco en el escaso panorama bibliográfico español.

Rafael González-Tablas y Sastre
Universidad de Sevilla, Octubre de 1997

INTRODUCCIÓN

La reflexión acerca de los derechos fundamentales ha adquirido en la hora presente una importancia capital. En los umbrales de un nuevo milenio creo necesario plantearse cual es el nivel efectivo de protección alcanzado por las personas en sus derechos más elementales, cúales las tensiones y peligros a los que se hallan sometidos, cúales las mutaciones que se han producido.

Por que si hay un aspecto que pueda caracterizar la actual configuración social y cultural es el de la evolución constante, la superposición de unas estructuras y sistemas de manera tan rápida, que es difícil, en ocasiones, captar su verdadera naturaleza, y su aportación al proceso de desarrollo humano.

Pero junto a esta rápida evolución, observamos, a modo de reverso de una misma moneda, el mantenimiento de viejas estructuras y sistemas, anquilosadas en sus antiguos ideales y presupuestos, y que no han sabido o no han podido adaptarse a los apremios de los nuevos tiempos. Sus antaño válidas e incluso generosas aportaciones a la resolución de los problemas de los hombres y de los grupos en que se integran se muestran hoy inoperantes para resolver los nuevos desafíos.

Las relaciones entre los nuevos avances tecnológicos y el Derecho son un buen ejemplo de esa tensión que acabamos de indicar.

Las innovaciones tecnológicas han supuesto un replanteamiento de las relaciones del hombre con el mundo, con el resto de los hombres, e incluso consigo mismo. Su acción no se limita a una mejora de nuestra calidad de vida o de nuestro bienestar; sino que va más allá, propiciando profundas transformaciones en el modo de entender nuestras sociedades, su organización y estructura. Surgen así nuevas realidades, que incorporan nuevas problemáticas, y cuya resolución sólo podrá operarse correctamente articulando nuevos mecanismos de tutela y garantía.

Por su parte, el Derecho, como elemento ordenador de la realidad, debe tener en cuenta los cambios operados en la misma, por cuanto cualquiera de ellos le afecta y origina adaptaciones y constantes transformaciones. Y es aquí donde surgen las fricciones. Las antiguas estructuras jurídicas no sirven, en numerosos casos, para solucionar los problemas planteados por los avances tecnológicos. Pero el Derecho tampoco debe quedar inerme ante este fenómeno, que está llamado a regular en defensa de los derechos e intereses de los ciudadanos. No debe olvidarse, que las nuevas tecnologías no sólo incorporan ventajas, sino también inquietantes amenazas.

Ante esta tensión - tecnología *versus* Derecho - dos cuestiones nos asaltan inmediatamente:

1. La necesidad de una adecuada ordenación jurídica de las nuevas tecnologías.
2. Los peligros que para los derechos fundamentales de los ciudadanos comporta un abuso o un uso torticero de las innovaciones tecnológicas.

Múltiples han sido las formulas ensayadas para lograr una correcta superación de este "enfrentamiento". Podemos adelantar ya que ello implicará , por un lado, una evolución tecnológica que no olvide la componente humana a cuyo servicio se manifiesta; por otra, una adaptación de las estructuras jurídicas a las nuevas exigencias, lo cual implicará una remodelación de los mecanismos de garantía, o su sustitución por otros adaptados a las nuevas necesidades protectoras. Es esta una de las preguntas que asalta hoy a la Teoría y la Filosofía del Derecho: ante nuevas agresiones contra los derechos fundamentales cometidos por medios tecnológicos, ¿ basta con una remodelación de los mecanismos de garantía ya existentes ?, o ¿ son necesarios nuevos instrumentos de tutela para hacer frente a las nuevas amenazas ?

A todas estas cuestiones intentaremos dar respuesta a lo largo de nuestra exposición. Por ahora sirvan como interrogantes que guiarán nuestro itinerario intelectual.

La cuestión de los derechos fundamentales no se agota actualmente, no obstante, en sus relaciones con el fenómeno tecnológico, sino que se ve sometida a una nueva perspectiva debido a la progresiva afirmación de la necesaria internacionalización de su reconocimiento y garantía.

Internacionalización que no sólo se manifiesta a través de las proposiciones elaboradas por organismos internacionales de nivel cuasiplanetario, tales como la Organización para las Naciones Unidas; si no que también se constata al nivel de las denominadas organizaciones regionales, cuyos ejemplos más próximos los tenemos en el Consejo de Europa y la Unión Europea.

Son precisamente estas últimas organizaciones las que por su limitación geográfica y concretos objetivos más se acercan e influyen en la vida de los ciudadanos de los Estados miembros. Sin embargo, los intereses de los ciudadanos no siempre son tenidos en cuenta a la hora de adoptar las grandes decisiones. Intereses económicos, políticos y/o estratégicos priman sobre la defensa de los derechos e intereses de los ciudadanos. Ello incorpora como consecuencia que el debate sobre el estatuto de los derechos fundamentales se obvia y queda reducido a una cuestión menor o testimonial.

De inmediato, nos asalta una nueva cuestión: ¿ cómo puede construirse un duradero de sistema de cooperación política y económica obviando a los ciudadanos, que son a la postre detentadores y destinatarios últimos del sistema ? La problemática en torno al reconocimiento y garantía de los derechos fundamentales a nivel "comunitario", queda reducida a la suma de las soluciones nacionales, a un estudio más o menos profundo de Derecho comparado, pero no, como sería de suyo, a la elaboración de una política común de defensa y garantía de los ciudadanos frente a los eventuales abusos que puedan cometerse en el seno de la organización común que se pretende articular. Si hablamos de intereses, problemas y soluciones comunes, al margen de localismos y soberanías trasnochados, ¿ porqué no hablamos de un reconocimiento y defensa unitarios de los derechos fundamentales ? El proceso tendente al reconocimiento y salvaguarda del derecho a la libertad informática a nivel comunitario ilustra convenientemente estas inquietudes.

Partiendo de estos presupuestos, y de su interrelación, hemos creído conveniente dividir nuestra exposición en dos partes.

→ La primera está dedicada a la determinación del estatuto del derecho a la libertad informática, como principal manifestación de la imbricación entre tecnología y ciencia jurídica en el campo de los derechos fundamentales. Para ello será necesario detenerse en cual sea su naturaleza jurídica, las facultades que lo conforman y las limitaciones a las que puede ser sometido. Todo ello con el horizonte de la polémica doctrinal y las enfrentadas posiciones que, sobre todo en la dogmática española, constituyen uno de los campos de debate más fructífero e interesante de la moderna Filosofía del Derecho.

Indicar, por último, que las cuestiones relativas a los instrumentos de garantía y a las limitaciones del derecho a la libertad informática son abordados de una manera fundamentalmente referencial. La enorme cantidad de reflexiones que suscitan y lo amplio de su problemática constituría *per se* el objeto de una concreta y exhaustiva investigación, que excede, con mucho, nuestro estudio.

→ La segunda de ellas se centra en la protección de los datos personales en el ámbito de la Unión Europea.

Aún no conceptuándose como Derecho comunitario, en el sentido estricto del término, los Acuerdos de Schengen, aplicados por una buena parte de Estados comunitarios, aportan importantes indicaciones acerca de como se manifiesta la protección de los datos personales en el ámbito supranacional europeo. La creación por el Acuerdo de 1990 de un Sistema de intercambio de información constituye el eje en torno al cual giran las potestades de los países signatarios en esta materia, así como las garantías que para los derechos de los ciudadanos deben inexcusablemente respetarse.

Ya en el nivel propiamente comunitario, la recien aprobada Directiva 95/46/CE, 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, constituye el último eslabón de una larga serie de intentos por establecer un equilibrio entre las exigencias de una mercado único, sin fronteras, y la libre circulación de datos personales de un Estado miembro a otro, con la protección de los derechos fundamentales de las personas. Pero para que ello sea posible se requiere que el tratamiento automatizado de datos personales sea equivalente en todos los Estados miembros, lo cual implicará, como señala la propia Directiva, una intervención de la Comunidad para conseguir la aproximación de las legislaciones nacionales. Los contenidos de esta Directiva serán objeto de un detenido estudio.

Nuestra exposición ha pretendido, de este modo, unir las formulaciones y planteamientos puramente teóricos con la realidad jurídica y sus productos normativos.

En lo tocante a fuentes de influencia señalar nuestra preferencia por aquellos trabajos que, a nuestro modesto criterio, han participado con suficiente altura científica en el debate sobre esta materia. Amén de la amplia, profunda e indispensable producción científica de Pérez Luño, merecen también destacarse los trabajos de Denninger, Frosini, Lucas Murillo de la Cueva, Ripoll, Simitis y una serie de aportaciones ya clásicas de un largo elenco de autores pertenecientes a la doctrina francesa.

En el campo del Derecho comunitario, señalar mi deuda con la obra de Carrillo Salcedo. Tampoco podría dejar de mencionar las aportaciones, entre otros, de Alonso García, Isaac, Louis, Häberle, Pérez Vera...

Esperemos poder cumplir nuestros objetivos inicialmente planteados, deteniéndonos para ello en una de las complicadas sendas a través de las cuales en la hora presente se manifiesta el Derecho. Siendo abundantísimas las fuentes bibliográficas sobre estas materias, se constata en un gran número de ellas una falta de preparación y rigor teórico, que justifican la mediocridad y desconocimiento en el tratamiento, que en numerosas ocasiones, se da a estas cuestiones. Es por ello que una de las tareas centrales de esta investigación ha consistido precisamente en realizar una criba teórica para deslindar las aportaciones valiosas de aquellas cuyo contenido debe juzgarse irrelevante; bien por sus deficiencias metodológicas o por los confuso de sus contenidos; bien por ser puras reiteraciones, cuando no plagios, de publicaciones anteriores. No se entienda lo afirmado como una muestra de petulancia o engreimiento, pues somos conscientes de nuestras limitaciones y carencias. Tal vez sea una manera poco adecuada de expresar nuestra fascinación e interés por este tema desde los lejanos tiempos de la Licenciatura por tierras extremeñas.

Es obligado, finalmente, rendir testimonio de gratitud a todas aquellas personas que me han apoyado en este caminar. A María Luisa, por el cariño que pone en todo lo que hace. Igualmente a Sebastián de la Obra, por su siempre paciente y

sincera ayuda. A Arancha, por su inestimable ayuda en la ordenación del material bibliográfico. Y a Margarita Prieto, del Centro de Documentación Europea de Sevilla, por mantenerme siempre al día de todas las novedades.

Mención especial para los Profs. González-Tablas y Sastre y Sánchez Jimenez y demás compañeros del Departamento de Filosofía del Derecho de la Universidad de Sevilla por su constante estímulo, sus palabras de aliento y sus consejos que tanto me han ayudado.

Para concluir, quiero rendir homenaje de reconocimiento y sincero agradecimiento a mi maestro D. Antonio E. Pérez Luño. No sólo por su magisterio constante, sus siempre sabios consejos y su infinita paciencia, si no también por haberme introducido en la senda del conocimiento y por tantas cosas que he aprendido desde que allá por 1992 tuve el enorme privilegio de empezar mi formación bajo su sabia dirección.

PRIMERA PARTE

EL DERECHO A LA LIBERTAD INFORMÁTICA

1. LA SOCIEDAD DE LA INFORMACION.

Las tecnologías de la información y las comunicaciones están generando en todo el mundo una nueva revolución industrial comparable en importancia y profundidad a sus predecesoras.

Es una revolución - *revolución digital*, se le denomina en determinados ámbitos - basada en la información, que es en sí misma expresión del conocimiento humano [1].

Esta situación nos lleva a los inicios de una nueva era: la de la información y la comunicación, en el seno de lo que se denomina como *"sociedad de la información"* [2].

Desde los años 70, los progresos de la tecnología se han manifestado con especial fuerza en el campo informático, caracterizándose por una explosión del número de ordenadores, el desarrollo de su capacidad de almacenamiento, una reducción de sus costes y una penetración creciente en los hogares, las empresas y la administración. Este proceso ha corrido paralelo al desarrollo del sector de las telecomunicaciones, que ha permitido una difusión ingente de informaciones a grandes distancias, creando toda una nueva gama de servicios telemáticos y de posibilidades de interconexión planetaria.

[1] Comisión de las Comunidades Europeas, Europa en marcha hacia la sociedad de la información. Plan de actuación, COM(94) 347 final, Bruselas, 19.07.1984, p. 3.

[2] De entre la numerosa producción científica sobre este aspecto pueden destacarse, entre otros: PEREZ LUÑO, A.E., *Nuevas tecnologías, Sociedad y Derecho. El impacto socio-jurídico de las nuevas tecnologías de la información*, Fundesco, Madrid, 1987; MASUDA, Y., *La sociedad informatizada como sociedad postindustrial*, trad. cast. de J. Ollero y F. Ortiz Chaparro, Fundesco & Tecnos, Madrid, 1984; NORA, S., y MINC, S., *La informatización de la sociedad*, trad. cast. de P. García de Pruneda y R. Ruza, Fondo de Cultura Económica, México-Madrid-Buenos Aires, 1980; ROMEO CASABONA, C.M., *Poder informático y seguridad jurídica*, Fundesco, Madrid, 1988; VITALIS, A., *Informatique, Pouvoir et Libertés*, Económica, Paris, 1981.

Para un consideración global de la sociedad de la información en el ámbito comunitario europeo, vid., COLOM, V., y VAN BOLHUIS, H.E., *Cyberspace reflections*, European Commission, DG XII y Social Research Unit, Brussels, 1995; cuyo original debo a la deferencia de Anne de Gref.

Hoy en día, el progreso técnico nos permite procesar, almacenar, recuperar y comunicar información en cualquiera de sus formas - oral, escrita o visual -, con independencia de la distancia, el tiempo y el volumen.

La información se ha convertido así en un medio tecnológico, formalizado jurídicamente, de enorme relevancia para la realización de múltiples actividades e iniciativas públicas y privadas [3].

En una sociedad cambiante como la nuestra, la ausencia de fuentes de información y las dificultades de comunicación entre los agentes sociales pueden dar lugar a la formulación de previsiones y juicios erróneos acerca de la realidad social del momento [4].

La revolución de la información está propiciando profundas transformaciones en el modo de concebir nuestras sociedades, en su organización y estructura. Efectivamente, se trata de una tecnología en constante evolución, cuyas capacidades aumentan día a día, su utilización se multiplica y diversifica sin cesar y traspasa las fronteras nacionales sin ningún obstáculo, con lo que significa para los hasta hoy consolidados principios de soberanía de los Estados y de territorialidad del Derecho [5].

Esto plantea un doble reto: aprovechar las ventajas inherentes a este nuevo proceso y hacer frente a los riesgos que de él se derivan, o asumirlo sin más y movernos en el mundo de la incertidumbre y el desasosiego.

Pero el desarrollo tecnológico no se manifiesta de manera ideal, pues junto a innegable progresos y mejoras, ha puesto en evidencia fenómenos de agresión a los derechos y libertades de los ciudadanos [6].

En las sociedades informatizadas del presente el poder no reside ya en el ejercicio de la fuerza física, sino en el uso de informaciones que permiten influir y controlar las actividades de los ciudadanos. De ahí que las posibilidades de intervención en los procesos sociales, económicos y políticos se determinen realmente

[3] Cfr. TORNE-DOMBIDAU JIMENEZ, J. y CASTILLO BLANCO, A., "Informática y protección de la privacidad del individuo (I)", en *Actualidad Administrativa*, núm. 22, 21 mayo-6 junio 1993, p. 270.

[4] Cfr. ALVAREZ-CIENFUEGOS SUAREZ, J.M., "La transferencia electrónica de información en la Comunidad Económica Europea", en *Actualidad Jurídica Aranzadi*, núm. 37, 23 de enero de 1993, p. 1.

[5] Cfr. CARRILLO SALCEDO, J.A., *Soberanía de los Estados y derechos humanos en Derecho Internacional contemporaneo*, Tecnos, Madrid, 1995; y ROMEO CASABONA, C.M., *Poder informático y seguridad jurídica*, cit., p. 16.

[6] Cfr. PEREZ LUÑO, A.E., "La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo", en *Anuario de Derechos Humanos*, núm. 4, Madrid, 1986-87, p. 259.

por el acceso a la información. La información deviene poder y ese poder se hace decisivo cuando transforma informaciones parciales y dispersas en informaciones en masa y organizadas [7]. Se manifiesta así, la necesidad de una regulación jurídica de este proceso, que conjugue el desarrollo tecnológico y científico, con la inexcusable defensa de los derechos y libertades de los ciudadanos.

1.1. *Las repercusiones jurídicas y sociales de la sociedad de la información.*

El Derecho surge de la realidad y vive en ella. Toda alteración en la misma le afecta y origina adaptaciones y transformaciones constantes [8]. Y que duda cabe que el proceso tecnológico que nos ha tocado vivir redimensiona el papel de la realidad y nuestro lugar en él. Se nos invita al consumo de informaciones diversas, pero sin participar en su elaboración y control; relegándonos así, como ha señalado Pérez Luño, a "meros suministradores de datos" [9].

Múltiples son las dimensiones que, para los diferentes ámbitos de la actividad humana, tiene el problema de la informatización de la sociedad; y múltiples también los enfoques planteados para otorgarles una correcta explicación [10].

De esta forma, observamos como bajo la imperiosa necesidad de "informatizarse" el número de adeptos incondicionales al proceso de informatización se multiplica cada vez más. Para ellos la informatización es la solución, que puede resolver de una vez para todas y para siempre todos los males que aquejan a la sociedad actual. Enfrente, los detractores del sistema, los que auguran la aniquilación del

[7] Cfr. PEREZ LUÑO, A.E., "Nuevos Derechos Fundamentales de la era tecnológica: la libertad informática", en *Anuario de Derecho Público y Estudios Políticos*, núm. 2, 1989/90, p. 172; ID, *Derechos Humanos, Estado de Derecho y Constitución*, 5ª edic., Tecnos, Madrid, 1995, p. 347.

[8] Cfr. LUCAS MURILLO DE LA CUEVA, P., "La protección de los datos personales ante el uso de la informática", en *Anuario de Derecho Público y Estudios Políticos*, núm. 2, 1989/90, p. 153. Estas tesis han sido desarrolladas posteriormente en sus obras: *El derecho a la autodeterminación informativa. La protección de los datos personales frente al uso de la informática*, Tecnos, Madrid, 1990; e *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993.

[9] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho...*, cit., p. 347.

[10] Son especialmente significativos, de entre su numerosa producción científica, los trabajos de PEREZ LUÑO acerca de: *Nuevas tecnologías, Sociedad y Derecho. El impacto socio-jurídico de las nuevas tecnologías de la información*, cit.; ID, "Implicaciones socio-jurídicas de las nuevas tecnologías de la información", en la obra colectiva Implicaciones socio-jurídicas de las nuevas tecnologías de la información, CITEMA, Madrid, 1991, pp. 273-290.

Asimismo, FROSINI, V., "Problemas jurídicos de la Información y la Documentación", en la obra colectiva Problemas actuales de la Documentación y la Informática Jurídica, ed. a cargo de A.E. Pérez Luño, Tecnos, Madrid, 1987, pp. 49-52; ID, "Las implicaciones sociales de la revolución informática: sus ventajas e inconvenientes", en Tecnologis, núm. 2, enero 1990, pp. 3-11; LOPEZ GARRIDO, D., "La sociedad informatizada y la crisis del Estado de bienestar", en Revista de Estudios Políticos, núm. 48, noviembre-diciembre 1985, pp. 27-45; NORA, S., y MINC, A., La informatización de la sociedad, cit.

hombre, la toma del poder por las maquinas, la supremacía del cerebro electrónico sobre la inteligencia humana [11].

La excesiva radicalización de ambas posturas, obvia cualquier consideración sobre su verdadera relevancia en el momento actual del debate acerca de la sociedad de la información. Por que cuando se habla de limitar la informática, no se pretende impedir su uso, sino conjurar las amenazas que de su uso pudieran derivarse [12].

Como gráfica y acertadamente ha señalado Pérez Luño, no se trata de subirse al carro de los apocalípticos o de los integrados, sino de someter la utilización de la informática a unas garantías jurídicas [13].

Ante este panorama, dos premisas pueden ya señalarse claramente:

1. Los riesgos para los derechos y libertades de los ciudadanos derivados de un uso abusivo o torticero de las nuevas tecnologías de la información.
2. La necesidad de una regulación jurídica del fenómeno tecnológico, tendente a optimizar los beneficios y minimizar los riesgos que de su uso pudieran derivarse para los ciudadanos.

Entre los beneficios, se señala que las nuevas tecnologías ofrecen la perspectiva de una sociedad menos sujeta a la introspección, la inercia y la compartimentación. La posibilidad que presentan las nuevas tecnologías de agrupar recursos que antes se encontraban dispersos, genera una infraestructura con un potencial ilimitado de adquirir conocimientos, innovación y creatividad, que se manifestará en múltiples sectores [14].

[11] Para un estudio profundo y detallado de ambas posiciones y de sus principales manifestaciones, vid., PEREZ LUÑO, A.E., "La contaminación de las libertades...", cit., pp. 268-282. Vid. también MADRID CONESA, F., *Derecho a la intimidad, Informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984, pp. 23-ss.

[12] Cfr. LUCAS MURILLO DE LA CUEVA, P., "La protección de los datos personales...", cit., p. 153.

[13] Cfr. PEREZ LUÑO, A.E., "La contaminación de las libertades..., cit., pp. 282-286.

[14] Se habla de múltiples aplicaciones, que repercutirán positivamente sobre la calidad de vida de los ciudadanos, la creación de puestos de trabajo y de empresas. Entre estas aplicaciones destacan: 1. Teletrabajo; 2. Educación a distancia; 3. Red de universidades y centros de investigación, 4. Servicios telemáticos para las pequeñas y medianas empresas; 5. Gestión del tráfico por carretera; 6. Control del tráfico aéreo; 7. Redes de asistencia sanitaria; 8. Licitación electrónica; 9. Red transeuropea de Administraciones Públicas; y 10. Autopistas urbanas de la información. El contenido y efectos de estas aplicaciones, referidos al ámbito de la Unión Europea, puede verse *en Europa y la sociedad global de la información. Recomendaciones al Consejo Europeo,* Bruselas, 26 de mayo de 1994, y en *Europa en marcha hacia la sociedad de la información. Plan de Actuación.* Comunicación de la Comisión al Consejo y al Parlamento Europeo y al Comité Económico y Social y al Comité de Regiones, COM(94) 347 final, Bruselas, 19.07.1994.

El principal riesgo reside en la creación de una sociedad a dos velocidades, compuesta por los que tienen y no tienen nada, en la cual sólo una parte de la población tenga acceso a la nueva tecnología, la maneje con soltura y goce plenamente de sus beneficios; en detrimento de sus conciudadanos.

Esta posibilidad, que ya se manifiesta por la concentración de determinados medios tecnológicos en manos de un numero reducido de manipuladores de la información, conlleva un estado de tensión, que se concreta en el temor y rechazo hacia esta "nueva sociedad" y sus instrumentos.

Esta situación plantea a las autoridades públicas la responsabilidad de establecer salvaguardias y de garantizar la cohesión de la nueva sociedad. Deberá garantizarse a todos un acceso equitativo a la información; la sociedad democrática reivindica el pluralismo informativo, así como el libre acceso y la libre circulación de informaciones [15].

Las potencialidades lesivas de los nuevos medios tecnológicos quedan claramente en evidencia cuando se ponen de manifiesto las posibilidades de las nuevas tecnologías, capaces de conseguir información detallada sobre individuos a partir de fuentes en forma de datos, voz e imágenes, y de manipular dicha información.

Los derechos fundamentales, especialmente el derecho a la intimidad, se ven así gravemente amenazados, ante las dificultades de resguardarse, de protegerse frente al control pormenorizado y riguroso de las nuevas tecnologías. Y es aquí donde el Derecho debe actuar serena, pero contundentemente, en la defensa de los derechos de los ciudadanos.

Como se apuntó anteriormente, no cabe asumir posturas radicales de sumisión o rechazo total. El ordenamiento jurídico no puede limitar su actuación a la prohibición o la aceptación, sin más; sino que debe ajustarse a las inquietudes, a las reivindicaciones del cuerpo social, de los ciudadanos que pueden verse agredidos por las nuevas tecnologías. Una sociedad cambiante exige un Derecho cambiante, un Derecho que se adapte a las nuevas demandas sociales [16]. Como ha señalado Alvarez-Cienfuegos, el ciudadano siente la necesidad de un derecho que no sea ineficaz, ni enloquecido; de un derecho que, en medio de los cambios sociales, refleje lo que él tiene de permanente e intangible en la regulación de la convivencia [17].

En definitiva, frente a la función social a que están llamadas las nuevas tecnologías de la información es preciso que el Derecho intervenga con el fin de diseñar y fijar las nuevas reglas del juego que se impone en la nueva sociedad en

[15] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho...*, cit., p. 346.

[16] Cfr. ROMEO CASABONA, C.M., *Poder Informático...*, cit., p. 16.

[17] Cfr. ALVAREZ-CIENFUEGOS SUAREZ, J.M., "La transferencia electrónica de información...", cit., p. 2.

transformación. Se impone la reflexión acerca de la posible conversión del ciudadano en un *"individuo transparente"*, y ello exige tomar las medidas convenientes para evitarlo.

2. LOS DERECHOS HUMANOS DE LA TERCERA GENERACION.

Los derechos humanos surgieron en la modernidad como respuestas a las exigencias éticas y los problemas políticos de aquella coyuntura histórica. Hoy, señala Pérez Luño, ese contexto ha variado profundamente, fruto de la revolución tecnológica [18].

Esta mutación contextual ha propiciado una reflexión en el ámbito jurídico, especialmente de la Filosofía del Derecho, acerca de las repercusiones de este proceso en el estatuto y configuración de los derechos de los ciudadanos; que no es más que una parcela de la preocupación global por definir el lugar que al hombre corresponde en el "nuevo mundo" que se pretende construir.

Ha llegado, en definitiva, el momento de preguntarse, como hiciera Frosini, ¿ hasta qué punto el actual desarrollo científico y tecnológico de la civilización humana permite establecer una relación con la "naturaleza humana", tal como ésta había sido concebida hasta el presente ?; y ¿ cuales de los viejos "derechos naturales" subsisten en la nueva situación ? [19].

Tras integrarse en un mundo nuevo, el de la sociedad tecnológica contemporánea, el individuo debe adecuar los ideales de antaño a la nueva realidad, y corresponde al filósofo del derecho cuestionarse si todavía habla del mismo Derecho al que hasta ahora se había referido [20], o si éste se presenta con nuevos rasgos, presupuestos y perspectivas.

2.1. *Las generaciones de derechos humanos: la dimensión histórica de los derechos humanos.*

Los derechos humanos, expresión que había representado durante siglos uno de los puntos más conflictivos en las discusiones entre los filósofos del derecho, surgen en la modernidad, en el seno del Iluminismo que inspiró las revoluciones burguesas, como respuesta jurídica a las exigencias y los problemas políticos y sociales de aquella época histórica [21].

[18] Cfr. PEREZ LUÑO, A.E., "Los derechos en la era tecnológica en la obra de Vittorio Frosini", en *THEORIA*, Vol. VII, núm. 16-17-18, tomo B, 1992, p. 1110.
[19] *Ibidem*, p. 1105.
[20] Cfr. FROSINI, V., "Los derechos humanos en la sociedad tecnológica", en *Anuario de Derechos Humanos*, núm. 2, 1983, p. 105.
[21] Cfr. PECES-BARBA MARTINEZ, G., *Tránsito a la modernidad y derechos fundamentales*, Mezquita, Madrid, 1982.

Los derechos humanos surgen con una marcado carácter individualista, como libertades particulares, tendentes a asegurar el conjunto de intereses individuales jurídicamente protegibles frente a la actividad del Estado. Es la consagración de la libertad en sentido negativo. Frente al progresivo incremento del aparato y del dominio estatal, el individuo sentía la necesidad de resguardar un espacio para sí, ajeno al control público y en el que pudiera desarrollar sus anhelos y expectativas [22]. Estas libertades individuales constituirían la *primera generación de los derechos humanos.*

Pero dicha concepción negativa de la libertad, esa impronta marcadamente individualista en la definición del estatuto de los derechos humanos, sufrió un amplio proceso de impugnación con ocasión de las luchas y reivindicaciones sociales del siglo XIX, fundamentalmente del proletariado, que puso de manifiesto la necesidad de un replanteamiento de la actividad estatal.

Las desigualdades sociales, las injusticias, la crisis del modelo económico liberal pusieron de manifiesto la necesidad de una intervención estatal redistribuidora de la riqueza, protectora de los más desfavorecidos; que tuviera en el ideal de la igualdad su valor guía. Se puso de manifiesto la necesidad de completar el catálogo de libertades individuales con una *segunda generación de derechos*, los derechos económicos, sociales, y culturales [23]. Ello requería una política activa de los poderes públicos encaminada a garantizar su ejercicio efectivo, cuya consagración política y jurídica tuvo lugar con la sustitución del Estado liberal de Derecho por el Estado social de Derecho [24].

Lo señalado pone de manifiesto como la mutación histórica de los derechos fundamentales ha propiciado la aparición de sucesivas "generaciones" de derechos. Y este proceso revela que es ésta una materia expansiva por naturaleza [25]. El dinamismo de los derechos humanos es una consecuencia de la tensión histórica entre factores socio económicos, culturales y políticos.

A lo largo del proceso evolutivo de la humanidad el desarrollo científico-tecnológico ha sido la respuesta histórica a los problemas concretos de cada época y contexto; a las cuestiones planteadas por las nuevas formas de relaciones sociales y por la ampliación constante de los anhelos y necesidades individuales y colectivas [26].

[22] Cfr. PEREZ LUÑO, A.E., *Los derechos fundamentales*, 3ª edic., Tecnos, Madrid, 1988, p. 32.
[23] Cfr. PEREZ LUÑO, A.E., "Nuevos derechos fundamentales de la era tecnológica: la libertad informática", en *Anuario de Derecho Público y Estudios Políticos*, núm. 2, 1989/90, p. 176.
[24] Cfr. PEREZ LUÑO, A.E., "Las generaciones de derechos fundamentales", en *Revista del Centro de Estudios Constitucionales*, núm. 10, septiembre-diciembre 1991, p. 205. *ID, Derechos Humanos, Estado de Derecho y Constitución*, 5ª edic., Tecnos, Madrid, 1995, pp. 219-229.
[25] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa. La protección de datos personales frente al uso de la informática*, Tecnos, Madrid, 1990, p. 34.
[26] Cfr. PEREZ LUÑO, A.E., "La defensa del ciudadano y la protección de datos", en *Revista Vasca de Administración Pública*, núm. 14, 1986, p. 44.

Estas nuevas necesidades son a la vez el precipitado de una consideración histórica del hombre y de sus derechos. Así se ha señalado como para Marx el alimento, vestido y vivienda constituían exigencias imprescindibles para la vida. Pero la satisfacción de esas necesidades no cerraba el proceso de satisfacción de las apetencias humanas, sino que, la satisfacción de esas necesidades primarias, la acción de satisfacerlas y las construcción de los medios necesarios para ello determinaban otras necesidades [27].

Por su parte Agnes Heller, una de los máximos representantes de la denominada Escuela de Budapest, ha señalado como una de las principales aportaciones marxianas la distinción entre *necesidades naturales* (medios que posibilitan la supervivencia material del hombre), *necesidades necesarias* (satisfacción de necesidades intelectuales, culturales de los hombres de una sociedad concreta en un período concreto) y *necesidades radicales* (opciones axiológicas orientadas hacia la plena y libre realización de la personalidad humana) [28].

Las necesidades radicales supondrán, en cuanto opción axiológica, la necesidad de alcanzar un consenso entre los diferentes miembros del cuerpo social acerca de qué objetivos deben alcanzarse, con qué medios y qué precio deberá pagarse por ello. Consenso que sólo será válido y efectivo, cuando todos los que participen en la adopción de las decisiones lo hagan en plano de igualdad, sin sometimiento de unos a otros; en definitiva, retomando de nuevo el ideario marxiano, en el seno de una sociedad plenamente desalienada.

La satisfacción de nuevas necesidades; esto es, las sentidas por la sociedad tecnológica, no debe hacerse, sin embargo, a cualquier precio. Y no debe hacerse, por que las nuevas tecnologías incorporan unos riesgos evidentes de agresión para los derechos ciudadanos. El acceso restringido y parcial de los ciudadanos a las informaciones necesarias para el libre desarrollo de su personalidad constituye, en la actual sociedad de la información, el ataque más flagrante a ese ideario de consenso *inter pares*, a esa sociedad libre donde los hombres puedan ser conscientes de la dignidad que les adorna y vivir de acuerdo a sus postulados.

La conciencia de esta realidad es la que ha propiciado un movimiento de reflexión en el mundo occidental acerca de los referidos riesgos de agresión y la

[27] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho...*, cit., p. 169, y la bibliografía allí citada.

[28] *Ibid.*, pp. 169-170. Sobre los principales representantes y aportaciones de la Escuela de Budapest al estudio de los derechos humanos, vid., HERRERA FLORES, J., *Los derechos humanos desde la Escuela de Budapest*, Tecnos, Madrid, 1989. Para una fundamentación antropológica de la teoría de las necesidades, vid., GONZALEZ-TABLAS SASTRE, R., "Necesidades y valores. Su fundamentación antropológica mediante una explicación heurística", en *Anuario de Filosofía del Derecho*, núm. 3, 1986, pp. 433-447.

necesidad de articular medidas para contrarrestarlos, y que tienen como denominador común la lucha por adaptar el estatuto de los derechos fundamentales a las exigencias de nuestro tiempo [29].

Así actualmente han surgido nuevas reivindicaciones (en su origen meras afirmaciones morales) cuyos instrumentos técnico-jurídicos son representativos de nuevas exigencias planteadas por las sociedades tecnológicamente desarrolladas.

La reivindicación de los derechos humanos en el momento actual se presenta con nuevas perspectivas, articulándose en torno a cuestiones tales como los derechos de los consumidores, el derecho al medio ambiente, el derecho a la calidad de vida y, especialmente, de libertad informática [30]. Junto a ellos se postulan también otros derechos de muy diversa naturaleza, tales como: las garantías frente a al manipulación genética, el derecho a morir con dignidad, el derecho al disfrute del patrimonio histórico y cultural, el derecho al cambio de sexo, etc...

Se plantea así la cuestión de si nos encontramos ante una *tercera generación de derechos humanos*, complementadora de las fases anteriores [31].

Hacen así su aparición formas nuevas de derechos humanos que eran desconocidas por las sociedades anteriores. Derechos que se presentan como una respuesta al fenómeno de la *"contaminación de las libertades"*, término con el que se alude a la erosión y degradación que sufren los derechos humanos ante determinados usos de las tecnologías [32].

Las innovaciones tecnológicas han propiciado un redimensionamiento del papel del hombre en el mundo; no sólo en la consideración de su entidad física, sino también del sistema de valores que guía su actuación y le hace avanzar. Por que, como ha señalado Frosini, para todos los teóricos del Derecho había hasta la edad moderna algunos principios reputados perfectamente conformes a la naturaleza

[29] Cfr. PEREZ LUÑO, A.E., "La contaminación de las libertades en la sociedad informatizada...", cit., p. 259.

[30] Frosini señala también como derechos humanos de la sociedad tecnológica: la abolición de las discriminaciones sociales y del trabajo forzado; la paridad de derechos entre hombres y mujeres, los derechos de los niños, minusválidos, retardados mentales, apátridas, refugiados, desnutridos; el derecho al secreto en la sociedad informatizada y el derecho a la información en la sociedad tecnológica. Cfr. FROSINI, V., *Cibernética, Derecho y Sociedad*, trad. cast. a cargo de C.A. Salguero-Talavera y R.L. Soriano Díaz, y Prólogo de A.E. Pérez Luño, Tecnos, Madrid, 1982; *ID*, "Los derechos humanos en la sociedad...", cit. pp. 105-ss.

[31] Cfr. PEREZ LUÑO, A.E., "Las generaciones de derechos...", cit., p. 206.

[32] Cfr. PEREZ LUÑO, A.E., "La libertad informática. Nueva frontera de los derechos fundamentales", en el vol. de M. LOSANO, A.E. PEREZ LUÑO y M.F. GUERRERO MATEUS, *Libertad informática y leyes de protección de datos personales*, Centro de Estudios constitucionales, Madrid, 1989, p. 144; SANCHEZ JIMENEZ, E., "Los derechos humanos de la tercera generación: la libertad informática", en *Actas del III Congreso Iberoamericano de Informática y Derecho* (Mérida, septiembre de 1992), publicadas en Informática y Derecho, núm. 4, 1994, pp. 165-ss.

humana, que hoy han sido sustituidos por principios totalmente opuestos, o sea, que se da una verdadera "transmutación de valores" [33].

2.2 *Rasgos innovadores de los derechos de la tercera generación.*

La tarea de precisar el catálogo de derechos de la tercera generación es una labor urgente y necesaria. Ello nos permitirá depurar que nuevos intereses reclamados por la ciudadanía incorporan nuevos derechos dignos de tutela y cuales sólo responden a meras modas o reivindicaciones pasajeras.

A esta labor puede contribuir el señalamiento de algunos rasgos caracterizadores de esta nueva generación de derechos.

Ha sido el Prof. Pérez Luño el que ha establecido la aportación doctrinal más depurada en este campo [34]. Siguiendo sus consideraciones, pueden señalarse como rasgos característicos de estos derechos los siguientes:

a. Fundamentación. Si la libertad sostuvo los derechos de la primera generación, y la igualdad los de la segunda, la *solidaridad* será el pilar de los de la tercera. Los nuevos derechos se hallan interrelacionados por su incidencia universal en la vida de todos los hombres. Sólo mediante un espíritu solidaria de *sinergía* - cooperación y sacrificio voluntario y altruista de intereses egoístas - será posible la satisfacción plena de las necesidades y aspiraciones comunes relativas a la paz, a la calidad de vida o a la libertad informática.

Frente a un "hombre sin atributos" de la primera generación, preten-didamente autónomo, en la tercera generación se profundiza en la idea ya existente en la segunda generación de un "hombre situado" en una circunstancia. Esto conlleva a una redimensión de la categoría de ciudadano y de libertad, que de ser libertades para uno mismo, pasan a ser libertades y derechos para con y en los demás derechos [35].

b. Instrumentos de tutela. La consideración histórico-generacional de los derechos humanos implica la correspondiente mutación de los mecanismos jurídicos que le sirven de reconocimiento y garantía.

Pérez Luño considera necesaria completar la teoría de los *status* de Jellinek [36]. A este respecto, debe considerarse el *status positivus socialis* como propio de los derechos de la segunda generación y otros dos tipos de *status* para los derechos

[33] Cfr. FROSINI, V., "Los derechos humanos en la sociedad...", cit., p. 105.
[34] Cfr. PEREZ LUÑO. A.E., "Las generaciones de...", cit., pp.209-217; *ID*, "Nuevos derechos fundamentales...", cit., p. 177.
[35] Cfr. PEREZ LUÑO, A.E., *Los derechos fundamentales*, cit., pp. 203-ss.
[36] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho...*, cit., pp. 87; *ID, Los derechos fundamentales*, cit., pp. 23-25.

de la tercera generación: el *status de habeas data*, para controlar y acceder a las informaciones contenidas en los bancos de datos [37], y el *status activus processualis*, que faculta a cada persona a participar activamente en los procedimientos que le afecten, constituyendo una forma de protección dinámica de los derechos frente al carácter pasivo que presentaba antes la protección de los mismos. Como afirma Pérez Luño, todo deviene procedimiento, y nos encontramos ante una nueva "proceduralización" en el derecho moderno; cuya importancia se halla corroborada por la difusión creciente de instituciones de protección que tienden a completar la función de garantía de los tribunales [38].

Así en las actuales sociedades tecnológicas, en las que la injerencia del ordenador en todos los aspectos de la vida del hombre se hace cada vez más amplia y agobiante, se aboga por el reconocimiento del derecho a la autodeterminación informativa, cuyo principal instrumento de garantía se concreta en el *habeas data*. Este nuevo cauce procesal para salvaguardar la libertad de la persona, y que significa en el ámbito de los derechos de la tercera generación lo que significó el *habeas corpus* para los derechos de la primera generación respecto a la libertad personal, consiste en la facultad de las persona en conocer y controlar las informaciones que les conciernen procesadas en bancos informatizados [39].

c. Titularidad. En la hora presente se asiste al reconocimiento de nuevas situaciones y posiciones jurídicas subjetivas. La experiencia de las últimas décadas ha mostrado que es necesario reconocer a la generalidad de los ciudadanos legitimación para defenderse de aquellas agresiones a bienes colectivos o intereses difusos que, por su propia naturaleza, no pueden tutelarse bajo la vieja óptica de la lesión individualizada. De este modo se han institucionalizado nuevos medios y estrategias para la defensa jurídica de intereses que no se pueden considerar privativos de una persona o un grupo, por incidir en la calidad de vida de los ciudadanos en su conjunto [40].

Igualmente conviene tener en consideración como otro rasgo particular de esta generación de derechos la reflexión adelantada por Frosini, cuando señala que, frente a los "derechos naturales" precedentes, éstos de la tercera generación no pueden ya calificarse de "innnatos". Por el contrario, están estrechamente vinculados a la sociedad tecnológica, en su calidad de derechos positivos [41]. Asume de esta manera una visión dinámica, histórica de los derechos humanos, que no puede limitarse a la formulación de los considerados "derechos clásicos", sino que debe responder a los apremios de la era que nos ha tocado vivir.

[37] Cfr. PEREZ LUÑO, A.E., *Nuevas tecnologías, sociedad y derecho*, cit. pp. 85-ss.
[38] Cfr. PEREZ LUÑO, A.E., "Las generaciones...", cit., p. 213.
[39] Cfr. PEREZ LUÑO, A.E., "Del Habeas Corpus al Habeas Data", en *Informática y Derecho*, núm. 1, 1992, pp. 153-161.
[40] Cfr. PEREZ LUÑO, A.E., "Nuevos derechos fundamentales de la era tecnológica...", cit., pp. 176-178.
[41] Cfr. FROSINI, V., "Los derechos humanos en la sociedad...", cit., p. 114.

2.3. *La polémica doctrinal en torno al reconocimiento de los derechos humanos de la tercera generación. A vueltas con la dimensión histórica y la necesidad de un catálogo abierto de derechos humanos.*

La consideración de los derechos de la tercera generación como auténticos derechos fundamentales constituye una de las heridas abiertas en el campo de la Filosofía del Derecho.

La impugnación por algún sector doctrinal de tal concepción nos coloca ante una primera disyuntiva: o se admite acríticamente como derechos fundamentales cualesquiera intereses, con lo que se puede perder precisión conceptual en esta categoría; o bien, se niega a esos intereses el rango de derechos fundamentales, se aboga por un férreo hermetismo conceptual, y se les ignora obviando su consideración de reivindicaciones humanas históricas.

De admitirse la primera proposición, podríamos encontrarnos con evidentes problemas de seguridad jurídica, de indefinición; en definitiva de minusvaloración del estatuto de los derechos fundamentales. El sometimiento a modas o criterios particulares egoístas en la reivindicación de determinados intereses no debe hacernos caer en la tentación de ampliación desorbitada e injustificada del catálogo de derechos.

Tal planteamiento podría conducirnos a la impugnación de su verdadero valor en las sociedades democráticas de nuestro tiempo, como núcleo vital que articula el sistema de garantías del Estado de Derecho, que toma en consideración de forma directa al individuo en tanto que ser humano que vive en sociedad. El Estado moderno, como organización política jurídicamente organizada, tiene su razón de ser en la realización de los derechos fundamentales [42].

Pero tampoco debe abogarse por una visión inmovilista, cerrada y definitiva del catálogo de los derechos fundamentales. Lo manifestado anteriormente no empece que determinados intereses si sean dignos de protección, que sea necesario su reconocimiento y su integración bajo el paraguas protector de los derechos fundamentales. Lo contrario supondría caer en la conclusión, ilusoria, de que el hombre ha alcanzado su plena realización, que sus reivindicaciones emancipatorias han tenido plena respuesta, y que ya nada precisa, pues todo está y le es satisfecho. Nuestra vida cotidiana nos demuestra día a día lo inasumible de tal conclusión.

El hombre se desenvuelve y desarrolla en un marco socio-temporal determinado, que mediatiza sus necesidades y los mecanismos de los que se vale para satisfacerlas. Las necesidades de ayer no son las de hoy; las de hoy no serán ya las de mañana. Si difícilmente puede entenderse al hombre fuera de su decurso histórico, imposible será determinar el estatuto de sus derechos si asumimos una consideración ahistórica, estática y cerrada de los mismos; que en nada casa con la manifiesta inquietud del espíritu humano.

La no asunción de estas constataciones en el campo de la reflexión jurídica se traduciría en un divorcio entre una estructura social sometida a constantes cambios y unas categorías jurídicas que permanecen ancladas en el pasado [43].

La naturaleza, e incluso la propia existencia, de los derechos humanos de la tercera generación ha sido objeto en los últimos años de una sabrosa polémica en la doctrina patria [44], cuyos argumentos pueden sintetizarse en torno a una doble, pero interrelacionada, problemática.

2.3.1. A vueltas con la historicidad de los derechos humanos.

Corresponde a Laporta el haber postulado unos derechos humanos descontextualizados, desvinculados de instituciones éticas, y que tengan como referente último la verdadera esencia del hombre; haciendo abstracción de los rasgos experienciales o de los contextos vitales propios de cada uno de los miembros individuales de una sociedad. Sólo así podrá predicarse el carácter universal de los derechos humanos (los derechos humanos se adscriben a todos y cada uno de los miembros individuales de la clase ser humano, al margen de circunstancias o planteamientos sociales, culturales o históricos ("roles" en la denominación laportiana); que junto al carácter absoluto (en cuanto expresión de intereses particularmente relevantes para los seres humanos) e inalienable (la formulación de los derechos humanos significa que no podemos pensar en ello como algo que pueda ser renunciado por la propia voluntad del titular) constituye la triada caracterizadora de los derechos humanos [45].

Esta consideración ha sido objeto de una abierta impugnación cuando se pone de manifiesto, como señala certeramente Pérez Luño, el riesgo de soslayar el soporte antropológico de los derechos humanos, cuya manifestación actual es el resultado de un proceso histórico de mutación [46]. La dimensión histórica del Dere-

[42] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., p. 17.

[43] Cfr. PEREZ LUÑO, A.E., "Introducción a los sistemas informatizados de documentación jurídica", en la obra colectiva, ed. a cargo de A.E. Pérez Luño, *Problemas actuales de la documentación y la informática jurídica* (Actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986), Tecnos & Fundación Cultural Enrique Luño Peña, Madrid, 1987, p. 31.

[44] Nos referimos a la polémica sustentada fundamentalmente entre el Prof. Laporta, por un lado; el Prof. Pérez Luño, por otro, y los Profs. Atienza y Ruiz Manero, en una tercera postura; y que encontró su plasmación en las páginas de la Revista *Doxa* durante 1987. Sus argumentaciones serán el hilo conductor expositivo de la cuestión en la doctrina española.

[45] Cfr. LAPORTA, F., "Sobre el concepto de derechos humanos", en *Doxa*, núm. 4, 1987, p. 32-ss.

[46] Cfr. PEREZ LUÑO, A.E., "Concepto y concepción de los derechos humanos (Acotaciones a la Ponencia de Francisco Laporta), en *Doxa*, núm. 4, 1987, p. 53-ss.

cho no supone por otra parte, como parece desprenderse de los temores señalados por Laporta acerca de la "inevitabilidad de la historia" [47], caer en un determinismo historicista, que condiciona irremisiblemente al hombre y sus manifestaciones. Pero tampoco supone asumir una mutación constante de la naturaleza humana, una variabilidad sempiterna que impida al hombre reconocerse en sí mismo, y que haga del Derecho pura regulación temporal necesitada de constante mutación.

Ambos elementos - dimensión histórica y naturaleza humana - lejos de ser contrapuestos, son plenamente complementarios. Y así la experiencia jurídica pertenece a la naturaleza y a la historia del hombre. De ahí que el hombre, al avanzar hacia el mundo nuevo, sigue siendo él mismo , que vive en un tiempo diverso, y que se hace diverso en un mundo que continúa siendo el mundo del hombre.

Huyendo del determinismo de la historia, cae Laporta en un determinismo axiológico, que llega incluso a negar al hombre el control sobre la disponibilidad de sus derechos, sus posibilidades de autodeterminación ("los derechos humanos, en tanto en cuanto son "inalienables", se le adscriben al individuo al margen de su consentimiento, o contra él, y se le inmuniza moralmente incluso frente a su propia voluntad", afirma[48]), rememorando aquellas coordenadas iusnaturalistas menos sensible a la historia, y a la proyección que en ella tiene el hombre.

Hoy, como ha señalado Frosini, la moderna consideración de los derechos humanos encuentra su norte en la contraposición entre los antiguos "derechos naturales", de los cuales se daban formulaciones de carácter estático y antihistórica, y los nuevos derechos humanos, que están caracterizados por su dimensión histórica y por su evolución y expansión continua y veloz [49].

A este respecto, reitera Pérez Luño, como frente al derecho natural ahistórico, la tesis iusnaturalista que sigue manteniendo validez es aquella que concibe el derecho natural como instancia crítica y valorativa de la experiencia jurídica en la historia [50].

Las prevenciones e intentos totalizadores de Laporta encuentran, tal vez, su justificación en una visión tremendista de la historia; como un caballo desbocado, que sólo se detiene cuando, por su propio esfuerzo, cae desfallecido. Ese "correr desbocado" conllevaría una sustitución global de estructuras; que, en el

[47] Cfr. LAPORTA, F., "Respuesta Pérez Luño, Atienza y Ruiz Manero", en *Doxa*, núm. 4, 1987, p. 76.
[48] Cfr. LAPORTA, F., "Sobre el concepto de derechos humanos", cit., p. 44.
[49] Cfr. FROSINI, V., "Los derechos humanos en la sociedad tecnológica", cit., p. 108.
[50] Cfr. PEREZ LUÑO, A.E., "Concepto y concepción de los derechos humanos", cit., p. 54.

tema que nos ocupa, supondría una mutación absoluta del estatuto de los derechos humanos.

Sin embargo olvida que, como ha señalado Pérez Luño, las generaciones de derechos humanos no implican la sustitución global de un catálogo de derechos por otro; sino que en ocasiones, se traduce en la aparición de nuevos derechos como respuesta a nuevas necesidades históricas (v.g. el derecho a la autodeterminación informativa frente a los riesgos de la sociedad informatizada), mientras que otras veces, supone la redimensión o redifinición de derechos anteriores para adaptarlos a los nuevos contextos en que deben ser aplicados [51].

2.3.2. La visión, abierta o cerrada, del catálogo de derechos humanos.

La asunción de una concepción generacional de los derechos humanos implica reconocer que el catálogo de las libertades nunca será obra cerrada y acabada. Una sociedad libre y democrática deberá manifestarse siempre abierta y receptiva a nuevas necesidades que fundamenten nuevos derechos [52].

El dinamismo de los derechos humanos es una consecuencia de la tensión entre factores sociales, económicos, políticos y culturales. Es por ello que estos derechos no pueden concebirse de una manera estática.

Los derechos de la tercera generación responden a la pretensión de satisfacer necesidades que la nueva sociedad tecnológica pone de manifiesto; por cuanto tienden a desarrollar, adaptándolos, necesidades, contenidos y pretensiones al principio no conocidos.

De esta forma, como señala Lucas Murillo de la Cueva, surgen primero como exigencias de la convivencia en un momento determinado. Cuando madura el convencimiento sobre su necesidad se pone en marcha un mecanismo de reivindicación ideológica y de reivindicación política que pretende su justificación. Esas reivindicaciones, legítima y democráticamente encauzadas, culminan en al asunción de nuevos derechos. Las formulaciones lingüísticas que los expresan son , a su vez, objeto de análisis, interpretación y comentario; cuyos presupuestos suelen ser las bases para el desarrollo de nuevos derechos. La interacción entre la realidad y sus productos normativos queda manifiesta en este proceso. [53]

Su fundamentación, de naturaleza claramente intersubjetivista, se halla en la concepción de los derechos humanos como valores intrínsecamente comunicables;

[51] Cfr. PEREZ LUÑO, A.E., "Las generaciones de derechos fundamentales", cit., p. 217; ID, "Concepto y concepción de los derechos humanos", cit., p. 56.
[52] Cfr. PEREZ LUÑO, A.E., "Las generaciones de los derechos humanos", cit., p. 217.
[53] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., p. 36-37. Vid. también, ARA PINILLA I., *Las transformaciones de los derechos humanos*, Tecnos, Madrid, 1990, especialmente pp. 137-150.

es decir, como categorías que, por expresar necesidades social e históricamente compartidas, permiten suscitar un consenso generalizado sobre su justificación [54].

Por que estos derechos no son impuestos, rogados o concedidos graciosamente; sino que son el resultado de una lucha, de una tensión creadora que conduce a un enriquecimiento de las situaciones jurídicas subjetivas que redunda en una creciente ampliación de las esferas de autonomía y participación de los individuos y sus grupos [55]. Y esa participación, esas reivindicaciones, en los sistemas democráticos, no serían posibles sin un consenso acerca de los valores y las necesidades; que nos indicaran las reglas del juego a seguir, y los ideales emancipatorios que pretendemos alcanzar.

Y no conviene olvidar que muchas de esas reivindicaciones no tienen ya un marco espacial concreto, sino que son sentidas a nivel planetario, poniendo de manifiesto la necesidad de un consenso global, superador de los particularismos y localismos en el reconocimiento, protección y defensa de los derechos humanos [56]. Nuevas necesidades para un nuevo orden mundial. Nuevas obligaciones, nuevos derechos.

El posicionamiento decidido a favor de una opción de *numerus apertus* en la determinación del catálogo de derechos humanos se revela necesario por la existencia de planteamientos reacios a admitir tal expansión.

Tal es la posición sostenida por Laporta, constituyendo el nudo gordiano de su argumentación, que se manifiesta en las primeras y últimas consideraciones del texto. Tras mostrar su alarma por la ligeras apelaciones que, según su criterio, se hacen a los derechos humanos y denunciar la multiplicación y diversificación de los derechos humanos, manifiesta: "y se anuncia todavía el nacimiento de una nueva "generación" de derechos relacionados con cosas tales como las nuevas tecnologías o la conservación de medio ambiente natural". Tal multiplicación se considera incompatible con la tendencia a "conferir a la idea de los derechos humanos una particular fuerza justificatoria o motivacional, como si se tratara de los escalones últimos y más poderosos de los sistemas morales y jurídicos, expresión de exigencias éticas y políticas tan fundamentales que no son susceptibles de negociación o trueque".

[54] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho...*, cit., especialmente pp. 162-176 y 527-540; Asimismo en "Concepto y concepción de los derechos humanos", cit., p. 63, donde en sus glosas a la Ponencia del Prof. Laporta señala: "... esos peculiares sistemas normativos que son los derechos humanos, no pueden ser aprehendidos a partir del estricto razonamiento lógico-deductivo, por que sus "relaciones justificatorias" pertenecen de lleno a la esfera del razonamiento práctico. De ahí, que estime que los modernos empeños rehabilitadores de la racionalidad práctica; las tesis neocontractualistas, así como la teoría consensual de los valores poseen incuestionable interés para abordar el significado y alcance de los derechos humanos".

[55] Cfr. LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa*, cit., p. 37.

[56] Para una visión de los derechos humanos en las nuevas relaciones internacionales, vid. el reciente trabajo de CARRILLO SALCEDO, J.A., *Soberanía de los Estados y derechos humanos en el Derecho Internacional contemporáneo*, Tecnos, Madrid, 1995.

La razón de tamaña contradicción estriba en el temor de "que cuanto más se multiplique la nómina de los derechos humanos menos fuerzan tendrán como exigencia, y cuanto más fuerza moral o jurídica se les suponga más limitada ha de ser la lista de derechos que la justifiquen adecuadamente" [57].

Es por ello que concluye recomendando que "haríamos bien en no trivializarlos apelando a ellos sin ton ni son o extendiendo los catálogos y las generaciones "arbitrariamente". De ello puede depender no sólo el que sean reconocidos, sino sobre todo el que sean efectivamente realizados en algún momento de la historia de la especie humana" [58].

Múltiples consideraciones nos sugiere esta peculiar versión del catálogo de los derechos humanos que, ya desde este momento, puede calificarse de peligrosamente restrictiva.

¿Cómo puede vincularse el efectivo reconocimiento y protección de los derechos humanos con un criterio cuantitativo de los mismos?; ¿ es que debemos conformarnos con los que tenemos?; ¿ No debe aspirar el hombre a mayores cotas de libertad y autorrealización?. Estas son, entre otras muchas, algunas cuestiones que la concepción laportiana plantea y que no encuentran una adecuada respuesta en su argumentación.

Tal tesis parece sugerir la necesidad de un peligroso conformismo del hombre hacia la reivindicación de sus derechos. Debemos conformarnos con lo que tenemos, no debemos osar reclamar más, so pena de perderlo todo y tener luego que lamentarnos. Asumamos la vieja sabiduría popular y subamos al carro de los que propugnan "más vale pájaro en mano que ciento volando".

Lo intolerable de tal conclusión es evidente, y pone de manifiesto la no consideración del proceso reivindicativo y consensual que da origen a los nuevos derechos. Éstos no surgen por un capricho de los ciudadanos, ni por las concepciones más o menos perfeccionadas de la doctrina científica. Surgen para colmar una laguna en las necesidades vitales del hombre, acallar su clamor ante la opresión tecnológica, acabar con el odio y la enemistad de los pueblos; en definitiva para que sí todos podamos disfrutar de todos los derechos. Y ello sólo puede hacerse adaptando la configuración y el número de los referidos derechos a las necesidades de un determinado contexto espacio-temporal en que el hombre se mueve. Porque, como ha señalado Pérez Luño, siguiendo a Denninger, la consideración

[57] Cfr. LAPORTA, F., "Sobre el concepto de derechos humanos", cit., p. 23.

[58] *Ibidem*, p. 44.

histórica enseña que los derechos fundamentales no son la expresión, ni el resultado de una elaboración sistemática de carácter racional y abstracto, sino respuestas normativas histórico-concretas a aquellas experiencias más insoportables de limitación y riesgo para la libertad [59].

Por otro lado, la prevención de no extender el catálogo de derechos humanos ante el temor de ver comprometida su efectiva realización, puede ser también objeto de abierta impugnación. La ampliación del catálogo de derechos humanos no desvirtúa necesariamente su concepto ni la fuerza jurídica que les es propia. Los derechos humanos no surgen al margen del sistema jurídico que los reconoce y les da cobertura; sino que gozan de los mecanismos de tutela y garantía que arropan a los demás derechos. De ahí que pueda afirmarse que, lo mismo que la libertad es indivisible, los derechos son interdependientes, se apoyan los unos en los otros reforzándose recíprocamente [60].

Es en el conjunto de garantías donde los derechos encuentran su fuerza, y donde constituyen, simultáneamente, el sustrato de nuevos mecanismos garantistas; en un proceso circular de mutua interdependencia. No es el criterio cuantitativo, sino el cualitativo el que determina la especial fuerza que acompaña al estatuto de los derechos humanos.

La consideración de los derechos fundamentales no sólo como expresión de posiciones jurídico subjetivas, sino como elementos esenciales del ordenamiento objetivo, pone de manifiesto este proceso de progresiva afirmación y ampliación de los derechos humanos. Los derechos asumen, así, una dimensión institucional a partir de la cual su contenido debe funcionalizarse para la consecución de los fines sociales y colectivos más relevantes [61].

La ampliación del número de derechos responde, consecuentemente, a la ampliación de las necesidades, de los objetivos y de las aspiraciones humanas. Pretender detener este proceso conllevaría a la negación de la historia y del papel que al hombre, como timonel, le corresponde en su decurso.

Lo hasta aquí señalado pone de manifiesto nuestra opción por un planteamiento generacional y abierto de los derechos humanos, que conjugue los ideales emancipatorios del hombre con la realidad concreta en la que nos movemos. Asumiendo el momento histórico en que nos movemos podremos encauzar nuestros anhelos, de una manera efectiva y práctica, hacia la consecución del ideario último: hacer de la libertad, la igualdad y la solidaridad algo real para todos los hombres.

[59] Cfr. PEREZ LUÑO, A.E., "Concepto y concepción de los derechos humanos", cit., p. 62.
[60] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., p. 38.
[61] Cfr. PEREZ LUÑO, A.E., *Derechos humanos, Estado de Derecho y Constitución*, cit., p. 300-ss.

Hasta que ese momento llegue la utopía seguirá teniendo plena vigencia, y la historia será el banco de pruebas del que las sucesivas generaciones humanas usarán para enjuiciar sus aportaciones a ese horizonte último.

Sirvan como corolario a lo hasta aquí apuntado lo manifestado por Pérez Luño, cuando certeramente señala: *"Faltos de su dimensión utópica los derechos humanos perderían su función legitimadora del Derecho; pero fuera de la experiencia y de la historia perderían sus propios rasgos de humanidad"* [62].

3. DE LA INTIMIDAD, COMO PRIVILEGIO INDIVIDUAL, AL RECONOCIMIENTO DEL DERECHO A LA LIBERTAD INFORMÁTICA.

3.1. *El reconocimiento del derecho a la intimidad.*

3.1.1. Planteamiento.

El establecimiento de un concepto general de la intimidad se manifiesta como una cuestión extremadamente difícil. Aunque para todos parece comprensible, se manifiesta imposible establecer una lista completa de todo aquello que, en cualquier sociedad, se puede considerar privado.

La aparición histórica del concepto jurídico de intimidad -como conjunto de facultades o poderes atribuidos a su titular - se halla, pese a haberse señalado momentos históricos más remotos, unida al surgimiento de la burguesía, y en la reivindicación de unas facultades destinadas a salvaguardar un determinado espacio con carácter exclusivo y excluyente[63].

La burguesía, protagonista de los avatares sociales, económicos y culturales de su tiempo, reclamaba un ámbito al margen de la injerencia estatal, e incluso de las propias relaciones sociales.

Este fenómeno se pone de relieve claramente en la distinción de Constant entre la libertad de los antiguos y la libertad de los modernos, que constituye, a su vez, el sustrato de la teoría de Berlin para la diferenciación entre libertad positiva y libertad negativa. La primera de estas libertades implica que "el individuo, soberano casi siempre en los asuntos públicos, era un esclavo en todas las cuestiones privadas"; mientras que la segunda supone que "el individuo independiente en su vida privada, no es soberano más que en apariencia, incluso en los Estados más

[62] Cfr. PEREZ LUÑO, A.E., "Las generaciones de derechos fundamentales", cit., p. 217.
[63] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho y Constitución*, cit., p. 321-ss. Para una consideración histórica de la intimidad, vid. también MARTINEZ DE PISON CAVERO, J., *El derecho a la intimidad en la jurisprudencia constitucional*, Civitas, Madrid, 1993, pp. 36-51.

libres". Los *modernos* sin renunciar a nuestras libertades políticas, ponemos sobre todo el acento en las individuales ("Nuestra libertad, señalaba Constant, debe componerse del goce pacífico y de la independencia privada") [64].

Ahora bien, esta actitud de recogimiento en la vida privada, conduce al riesgo, ya apuntado por Tocqueville, de un fortalecimiento desmesurado del poder único, uniforme y fuerte del Estado por el abandono de los ciudadanos de los asuntos públicos. De ahí que sea necesario un equilibrio, un punto intermedio entre lo íntimo y la participación política; entre el individuo y el Estado [65].

Esta atmósfera de pensamiento encontró su cauce de expresión años más tarde cuando, en el seno del pensamiento jurídico anglosajón, se sentaron las bases jurídicas de la noción de *privacy*. Su origen se halla en la formulación del juez Cooley en 1888 ("el derecho a que a uno le dejen en paz"); retomada posteriormente por Warren y Brandeis en un artículo que se anticipaba a su tiempo, "The Right to Privacy" (publicado en *Harvard Law Review*, en 1890), configurando la *privacy* como un derecho a la soledad, como la garantía del individuo a la protección de su persona y a su seguridad frente a cualquier invasión del sagrado recinto de su vida privada y doméstica [66].

Por su parte, en el ámbito del derecho continental europeo, la aportación a establecimiento de la noción de intimidad consistió en la construcción civilística de los derechos de la personalidad; que encuentran en la dignidad humana su principio legitimador. Como ha señalado certeramente Pérez Luño, la dignidad humana no sólo constituye la garantía negativa de que la persona va a ser objeto de ofensas o humillaciones, sino que entraña también la afirmación positiva del pleno desarrollo de la personalidad. La dignidad humana supone, así, el valor básico fundamentador de los derechos humanos que tienden a explicitar y satisfacer las necesidades de la persona en la esfera moral. De ahí que represente el principio legitimador de los derechos de la personalidad; entre los cuales se encuentra incluido el derecho a la intimidad [67].

Ambas aportaciones confluyeron en las grandes declaraciones internacionales de derechos que reconocen el derecho a la intimidad [68]. Asimismo en los

[64] Cfr. GARCIA SAN MIGUEL RODRIGUEZ-ARANGO, L. (edic. a cargo de), "Reflexiones sobre la intimidad como limite de la libertad de expresión", en la obra colectiva *Estudios sobre el derecho a la intimidad*, Tecnos & Universidad de Alcalá de Henares, Madrid, 1992, p. 15; LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., pp. 45-49.

[65] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., pp. 55-56.

[66] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho y Constitución*, cit., p. 323; MARTINEZ DE PISON CAVERO, J., *El derecho a la intimidad en la jurisprudencia...*, cit., p. 26.

[67] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho y constitución*, cit., pp. 318-ss, y la amplia bibliografía allí citada. Asimismo, ROGEL VIDE, C., *Bienes de la personalidad, derechos fundamentales y libertades públicas*, Publicaciones del Real Colegio de España, Bolonia, 1985.

[68] Art. 12 de la Declaración Universal de 1948; art. 17.1 del Pacto Internacional de Derechos Civiles y Políticos de 1966; y art. 8.1 de la Convención Europea para la protección de los Derechos Humanos y de las Libertades Fundamentales de 1950.

ordenamientos jurídicos internos se procede a la recepción constitucional del derecho a la intimidad. En el ámbito europeo, fue el art. 26.1 de la Constitución portuguesa el primero que se hizo eco del derecho a la intimidad. Posteriormente, la española de 1978 en su art. 18. Incluso en los ordenamientos jurídicos carentes de un pronunciamiento constitucional expreso, se ha procedido a su reconocimiento a través de otros preceptos constitucionales [69], y por su regulación legislativa y jurisprudencial [70].

Pero lo que no ha recogido ninguno de estos textos precitados es una descripción, ni siquiera aproximada, a diferencia de otros derechos incorporados en los textos, del derecho a la intimidad [71].

Una de las causas de esta definición deriva de la inexistencia de una idea clara de que sea intimidad, y que deba entenderse amparado bajo su manto protector. Se impone por lo tanto, como cuestión previa, un intento de depuración terminológica.

3.1.2. Delimitación Conceptual.

Todos los intentos de delimitar el significado de la intimidad parten con una dificultad previa: la inexistencia de un acuerdo generalizado sobre el término concreto a utilizar [72]. Se emplean por igual expresiones como "intimidad", "vida privada", "esfera privada", "privacidad", o se alude a "lo íntimo", "lo reservado". No debe olvidarse por otra parte, como advierte Pérez Luño, que las nociones de intimidad y vida privada llevan consigo una gran carga emotiva que las hace equívocas, ambiguas y dificulta la precisión de su significado [73].

Antes de adentrarnos en otras consideraciones, sí quisiéramos expresar nuestro desagrado por la reiterada utilización en la legislación y doctrina españolas del neologismo *privacidad*; término sin arraigo en nuestro lenguaje, y que no es más una

En el ámbito del Derecho Comunitario Europeo, destacan el art. 6 de la Declaración de los derechos y libertades fundamentales elaborada por el Parlamento Europeo en 1989; y en el núm. 6 del Título VIII del Proyecto de Constitución Europea, elaborado igualmente por el Parlamento Europeo, en su redacción de 1994. Además el TJCE ha manifestado que el respeto de la vida privada constituye un derecho fundamental protegido por el ordenamiento comunitario (Asunto C-62/90, Comisión vs. República Federal de Alemania, Rec. 1992-I).

[69] Sirvan como ejemplo: Alemania por referencia al art. 2 de la *Grundgesetz*; o Italia por referencia al art. 2 de la Constitución Italiana.

[70] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., pp. 74-75.

[71] Cfr. BERMEJO VERA, J., "Premisas jurídicas de la intimidad personal y de la protección de los datos en el Derecho español", en la obra colectiva *Libro Homenaje al Profesor José Luis Villar Palasí*, Civitas, Madrid, 1989, p. 150.

[72] Cfr. MARTINEZ DE PISON CAVERO, J., *El derecho a la intimidad en la jurisprudencia...*, cit., p. 28.

[73] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho y Constitución*, cit., p. 327.

traducción literal y simplista de la noción inglesa de *privacy*. Y aquí radica la gravedad de la confusión, por cuanto no se trata de una simple asunción lingüística de un término extraño a nuestro diccionario; sino de la equiparación de conceptuaciones de la intimidad que aparecen claramente diferenciadas en los sistemas de Derecho continental y del *Common Law*. Sin detenernos excesivamente en esta cuestión, el término privacy puede considerarse que comprende lo que para nosotros es "intimidad" y "vida privada", círculos concéntricos de distinta amplitud; si "vida privada" comprende, obviamente, lo que es íntimo no todo lo que es íntimo puede extenderse a "vida privada". Además en el mundo jurídico anglosajón se ha trazado una clara frontera entre el contenido de las nociones de *privacy e intimacy*. La primera hace referencia a la posibilidad de los particulares de controlar el acceso de extraños a lo que le es propio, sus circunstancias familiares o relaciones personales, así como a controlar también la posibilidad de que de todo ello se dé publicidad. El ámbito de la *intimacy* es mucho más restringido, haciendo alusión a las relaciones íntimas que se tienen con los otros, y, en particular, a las relaciones sexuales.

La cuestión, sin embargo, no se limita a una equiparación doctrinal errónea de términos claramente diferenciados; sino que va más allá, e incluso encuentra apoyatura en determinadas disposiciones legales. El paradigma de tamaño despropósito lo encontramos en el Derecho español, y concretamente en la Exposición de motivos de la LORTAD [74]. El legislador español, a modo de interpretación auténtica, establece y asume la noción de privacidad en el derecho patrio; relegando la intimidad a un sector más restringido. Y esto se hace sin ninguna base doctrinal, legal o jurisprudencial previa, sino sólo amparado en el snobismo de asumir como bueno lo extraño, y despreciar lo propio como algo obsoleto o inadecuado a las circunstancias presentes. Así se manifiesta el legislador español: " Notese 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". Posteriormente, no obstante su apuesta por la privacidad - que puede resultar menoscabada por la utilización de las tecnologías informáticas - recurre nuevamente, en una manifiesta y flagrante perdida de coherencia interna, al concepto de intimidad, al señalar la necesidad de delimitar una nueva frontera de la intimidad frente a la utilización mecanizada y discriminada de los datos personales. El sonrojo que produce y lo incoherente de esta "aportación" legislativa obvia cualquier otro comentario.

[74] Abreviatura de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, publicada en el BOE núm. 252, de 31 de octubre de 1992.

Hecha esta salvedad y al margen de diferentes nomenclaturas, el problema reside en determinar si, bajo cada denominación, nos estamos refiriendo a la misma cosa o a cosas diferentes.

3.1.3. La determinación de su contenido: del "*ius solitudinis*" a su dimensión social.

Múltiples han sido los intentos doctrinales por delimitar el contenido de la intimidad [75] , y múltiples las definiciones esbozadas. La mayoría llegaron a la conclusión de que el concepto de intimidad no podía ser definido de un modo satisfactorio. Las posibles definiciones, o son muy amplias, equiparando el derecho a la intimidad con el derecho a que a uno le dejen en paz, o se reducen a una lista de diversos valores a los que se puede aplicar el adjetivo de "íntimo" o "personal" de un modo razonable pero no exclusivo [76]. La relatividad del concepto de intimidad es, por tanto, evidente [77].

Podría considerarse la intimidad como la antítesis de lo público: por tanto, todo aquello relativo al hogar, la familia, la religión, la salud, la sexualidad y los asuntos legales y económicos personales de un individuo. Pero, el individuo es miembro de la sociedad y como tal no puede pretender disfrutar de una intimidad total. La formulación "el derecho a que a uno le dejen en paz" resulta demasiado simplista.

Esta noción filosófica de intimidad ha sido ya superada, pues no cabe circunscribirla a un *ius solitudinis*. La elaboración jurídica de la intimidad tiende a transportarla desde la esfera de la soledad a la de las relaciones sociales [78]. Debe partirse, consecuentemente, de la valoración de los distintos ámbitos de relación en los que actúa el individuo [79].

No obstante, como señala Pérez Luño, la concepción de la intimidad como aislamiento no es necesariamente incompatible con sus proyecciones sociales, si se la considera como un primer paso en su proceso formativo. La dimensión interna de la intimidad necesita para realizarse de un proceso de exteriorización, que entronca ya con la dimensión social del hombre y de sus manifestaciones. Se concluye así en

[75] Para una exposición concreta y rigurosa de estas aportaciones, vid. entre otros: PEREZ LUÑO, A.E., *Derechos humanos, Estado de Derecho y Constitución*, cit., pp. 327-331; MADRID CONESA, F., *Derecho a la intimidad, informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984, pp. 35-38; MARTINEZ DE PISON CAVERO, J., *El derecho a la intimidad en la jurisprudencia...*, cit., p. 30-31.

[76] Cfr. "Informe de la Comisión Calcutt sobre la intimidad y cuestiones afines", *Cuadernos del Consejo General del Poder Judicial*, núm. 4, 1991, p. 29.

[77] Relatividad que, siguiendo a Madrid Conesa, se manifiesta en cuatro apartados: 1. *Relatividad tempo-espacial*; 2. *Relatividad individual*; 3. *Relatividad social*; 4. *Relatividad normativa*. Cfr. MADRID CONESA, F., *Derecho a la intimidad, informática...*, cit., p. 41.

[78] Cfr. PEREZ LUÑO, A.E., "Dilemas actuales de la protección de la intimidad", en la obra colectiva, edic. a cargo de J.M. Sauca, *Problemas actuales de los derechos fundamentales*, Universidad Carlos III & Boletín Oficial del Estado, Madrid, 1994, p. 314.

[79] Cfr. MADRID CONESA, F., *Derecho a la intimidad, informática...*, cit., p. 39.

la consideración actual de la intimidad como categoría cultural, social e histórica [80], superadora de antítesis anteriores, y cuyo status presente puede condensarse en tres grandes notas:

a. La sustitución de la visión cerrada y estática de la intimidad por una concepción activa y dinámica en la que la intimidad se contempla como la posibilidad de conocer, acceder y controlar las informaciones que conciernen a cada persona.
b. La decantación legislativa hacia la componente externa y social de este derecho, con la asunción de la tutela jurídica de los "datos personales" y "perfiles de personalidad", que se proyectan como un conjunto más amplio y global de relaciones intersubjetivas.
c. La opción por un sistema de tutela de la intimidad basada en los valores e intereses, públicos o privados, que pueden contraponerse al deseo de la persona concernida de mantener sus datos en secreto [81].

3.2. *Intimidad e informatica: la nueva frontera.*

3.2.1. La intimidad en la sociedad informatizada: intimidad *versus* información.

No debe olvidarse que el contexto en que se ejercitan los derechos humanos es el de una sociedad donde la informática ha devenido el símbolo de nuestra cultura, hasta el punto de que para definir nuestro actual modelo de convivencia se alude a la expresión *sociedad informatizada* [82].

Ya se aludió anteriormente a los riesgos que para el disfrute de los derechos fundamentales pueden suponer determinados progresos tecnológicos; riesgos que se han hecho particularmente acuciantes en relación con el derecho a la intimidad [83].

El derecho a la intimidad ante el desarrollo tecnológico está generando formas, procedimientos y técnicas que permiten la intromisión en ese reducto de soberanía individual, sin que en muchos casos sea siquiera perceptible.

Cuando las inmensas posibilidades de la técnica no se aplican al servicio del hombre, sino para someterlo, la informática deviene una terrible amenaza para la libertad de los hombres, convirtiendo la sociedad en una inmensa casa de cristal en la que todas nuestras manifestaciones, nuestras grandezas y nuestras miserias, quedan al desnudo ante cualquier observador [84].

[80] Cfr. PEREZ LUÑO, A.E., "Dilemas actuales de la protección de la intimidad", cit., p. 315.
[81] *Ibídem*, pp. 315-318.
[82] Cfr. PEREZ LUÑO, A.E., "Intimidad y protección de datos personales: del *habeas corpus al habeas data*", en la obra colectiva, edic. a cargo de L. García San Miguel, *Estudios sobre el derecho a la intimidad*, Tecnos & Universidad de Alcalá de Henares, Madrid, 1992, p. 38.
[83] ID, *Derechos Humanos, Estado de Derecho y Constitución*, cit., p. 346.
[84] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., p. 108.

Los avances de la tecnología informática y de las telecomunicaciones han permitido la acumulación de un ingente volumen de datos personales antes inimaginable. De esta manera, datos antes dispersos aparecen ahora unificados en grandes bases de datos. Ello permite la elaboración de perfiles electrónicos de nuestra propia personalidad, como único dato válido y referencial para los demás individuos. Esta situación provoca que no esté en juego sólo la intimidad, sino que, como señala Lucas Murillo de la Cueva, es el derecho a la propia identidad el que corre peligro con el uso irrestricto y desordenado de las tecnologías de la información [85].

Pero ese acopio de información no es algo espontáneo. Las inquietudes hacia el conocimiento forman parte del ser del hombre desde que se conceptúa como tal. Su búsqueda es lo que ha hecho avanzar y sobreponerse a sus propias limitaciones físicas, innovando, modificando el espacio vital que le acoge, e incluso la propia percepción que tenemos del mismo. Lo que sí supone una novedad en la sociedad tecnológica es que la información, como señala Pérez Luño, se ha convertido en un auténtico poder. La posibilidad de acumulación ilimitada de un gran número de datos personales, de ordenación, recuperación inmediata y transmisión a grandes distancias ha generado una forma de dominio que era desconocido en etapas anteriores [86].

Pero junto a ese acopio informacional se evidencia en las sociedades democráticas desarrolladas y consolidadas una reestructuración de los objetivos de sus instituciones y de los derechos fundamentales que las justifican. Tras la consolidación de un nivel de vida digno, la sociedad y el Estado pierden interés y comienza la preocupación por uno mismo.

El hombre ya no está sometido a reglas uniformes, homogenizantes, en aras de la consecución de unos ideales colectivos; sino que surgen nuevos valores que impulsen el desarrollo de la personalidad íntima, de la libre configuración vital de cada individuo[87].

El valor predominante, la finalidad y el objetivo que fundamenta nuevas inquietudes es el respeto a la singularidad objetiva; es decir, el derecho a la intimidad, que no es más que el derecho a ser uno mismo. De ahí que el derecho a la intimidad, el derecho a un ámbito personal totalmente libre sea objeto de renovado interés en cuanto hecho social y cultural más significativo de nuestro tiempo, a la vez que constituya objeto de preocupación de teóricos y juristas por concretar

[85] *Ibídem*, p. 109.
[86] Cfr. PEREZ LUÑO, A.E., *Libertad informática y leyes de protección de datos personales*, en colab. con M.G. Losano y M.F. Guerrero Mateus, Centro de Estudios Constitucionales, Madrid, 1989, p. 138.
[87] Cfr. ROVIRA VIÑAS, A., "Reflexiones sobre el derecho a la intimidad en relación con la informática, la medicina y los medios de comunicación", en *Revista de Estudios Políticos*, núm. 77, julio-septiembre 1992, p. 260.

y garantizar su naturaleza ante los nuevos avatares a que se condiciona su propia existencia y reconocimiento.

No obstante estos nuevos perfiles de reivindicación de lo íntimo, la sociedad actual se mueve en torno a la existencia de un Estado fuertemente intervencionista, con unas exigencias prestacionales que la propia sociedad reclama. El progreso y la eficacia en la consecución de esas exigencias son facilitados por las nuevas tecnologías, que permiten un masivo acopio de datos personales acorde con las necesidades de intervención estatal. Pero ello es precisamente la causa de la actual revitalización del anhelo de intimidad, de preservación siquiera de un pequeño reducto de vida privada, al margen del omnímodo control estatal.

El dilema es evidente: si deseamos una acción eficaz de los poderes públicos debemos aceptar un libre flujo de informaciones, pero se corre el riesgo de relegar a los ciudadanos a meros "suministradores de datos"; o se ponen en peligro la consecución de determinados intereses públicos de eficacia y seguridad, si aceptamos que los ciudadanos deben estar protegidos frente a un uso indiscriminado de sus datos

De igual modo en el sector privado, convertido ahora en auténtico *sector cuaternario*, se ha producido una fiebre de acopio de datos. La información no sólo deviene poder, sino que incorpora unas plusvalías económicas para aquellos que la poseen y están dispuestos a transmitirla a otros a cambio de un precio. Se ha consolidado la mercadurización de la información. Las empresas nos agobian con ofertas múltiples y de los más variopintos sentidos. Ante esta situación, se ha abogado, especialmente desde el sector de los molestos mercaderes de la información y de los ofertantes de servicios, por una solución consistente en la inscripción en unos ficheros -denominados gráficamente como *ficheros Robinson* - de los ciudadanos que no quisieran recibir publicidad. Lo descabellado e insoportable de tal solución se pone de manifiesto cuando se asume la sabia reflexión elaborada por Pérez Luño sobre los riesgos inherentes a la asunción de tal inscripción. Señala este respecto: " Así se alude ahora a los denominados "ficheros Robinson" en los que deberían inscribirse aquellos ciudadanos que no quieran ver perforada su privacidad por la recepción de propaganda no deseada... Ya el nombre de esos ficheros denuncia parcialidad del juicio. Supone que el ciudadano normal es el que acepta gustoso la contaminación de su vida privada... El ciudadano insólito será aquel que se obstine en salvaguardar su derechos fundamental a la intimidad y se autoconfina en un aislamiento parangonable al sufrido por Robinson en su isla solitaria... *en un Estado de Derecho ningún ciudadano debe verse obligado a inscribirse en un archivo adicional de datos, para que sean respetados sus derechos y libertades* " [88]. Otro nuevo dilema a resolver.

[88] Cfr. PEREZ LUÑO, A.E., y de entre su numerosa producción científica sobre este extremo, los siguientes trabajos: "COMENTARIO LEGISLATIVO: LA LORTAD y los derechos fundamentales", en *Derechos y Libertades*, núm. 1, febrero-octubre 1993, p. 417; "La protección de datos personales en España: presente y futuro", en *Actas del III Congreso Iberoamericano de Informática y Derecho* (Mérida, septiembre de 1992), publicadas en *Informática y Derecho*, núm. 4, 1994, p. 241; "Dilemas actuales de la protección de la intimidad", cit., p. 321. El subrayado es nuestro.

Conviene también tener presente que la información, no obstante lo apuntado, también se manifiesta como una necesidad de la hora presente. La posibilidad de un acceso igualitario y pluralista a la información se constituye hoy como una exigencia ineludible. Tal es así que el derecho a la información se reconoce normativamente y se articulan garantías para su defensa.

Sin detenernos en esta problemática, no debe olvidarse que en los sistemas democráticos con un sistema protector de los derechos de los ciudadanos, las situaciones conflictivas es lógico que sean frecuentes en el despliegue real de su ejercicio; intimidad y libertad de expresión e información; interés público e interés privado; publicidad y secreto; reserva y transparencia. Hacer posible una convivencia en el ordenado ejercicio de esos derechos supone la correcta modulación de los intereses en conflicto, la determinación de su significación actual. Constituye una más que amplia problemática que el legislador, los Tribunales y la propia sociedad tienen que dilucidar [89].

Ahora bien, la correcta comprensión del estatuto actual de la intimidad no podrá lograrse sí antes no damos solución a los dos dilemas que dejamos planteados y que no se referían a otra cosa más que a las relaciones entre las necesidades de información - del sector público y privado - y el respeto de los derechos ciudadanos. Como señala Pérez Luño, las sociedades actuales precisan de un equilibrio entre el flujo de informaciones y la garantía de la intimidad de los ciudadanos. Ello sólo podrá lograrse mediante un adecuado ordenamiento jurídico de la informática, capaz de armonizar las exigencias de información propias de un Estado avanzado con las garantías de los ciudadanos [90].

[89] Para un estudio de las relaciones entre los derechos a la intimidad y a la información vid., entre otros: BUSTOS PUECHE, J.E., "Los límites de los derechos de libre expresión e información según la jurisprudencia", en la obra colectiva, edic. a cargo de L. García San Miguel, *Estudios sobre el Derecho a la intimidad*, Tecnos & Universidad de Alcalá de Henares, Madrid, 1992, pp. 101-156; DE MIGUEL CASTAÑO, A., *Derecho a la información frente al derecho a la intimidad. Su incidencia en el sistema de información estadística*, I.N.E., Madrid, 1983; ESPINAR VICENTE, J.M., "La primacía del derecho a la información sobre la intimidad y el honor", en la obra colectiva, *Estudios sobre el Derecho a la intimidad*, cit., pp. 46-67; GARCIA SAN MIGUEL RODRIGUEZ-ARANGO, L., "Reflexiones sobre la intimidad como límite de la libertad de expresión", *Ibid.*, pp. 15-35; KAYSER, P., *La protection de la vie privée*, Economica, Paris, 1984; MARTINEZ DE PISON CAVERO, J., *El derecho a la intimidad en la jurisprudencia...*, cit., pp. 136-146; O´CALLAGHAN MUÑOZ, X., *Libertad de expresión y sus límites, honor, intimidad e imagen*, Edersa, Madrid, 1991; OSORIO, L., "Los derechos al honor, a la intimidad y a la propia imagen como límites de la libertad de expresión e información, en la obra colectiva, *Los derechos fundamentales y las libertades públicas*, Ministerio de Justicia, Madrid, vol. I, pp. 659-689; PEREZ LUÑO, A.E., "Dilemas actuales de la protección de la intimidad", cit., pp. 323-330; RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalite*, Bruylant & L.G.D.J., Bruselas, 1990; VITALIS, A., *Informatique, pouvoir et libertés*, cit.

[90] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho y Constitución*, cit., p. 348.

3.2.2. La protección de los datos personales.

El derecho a la intimidad ha adquirido nuevos perfiles en la era tecnológica; hasta el punto de señalarse un *antes* y un *después* de la informática en cualquier consideración de la intimidad que quiera ser correcta [91].

La mutación tecnológica ha provocado un cambio en la consideración de la intimidad - hacía esa concepción social, cultural e histórica a la que antes nos referíamos -, hasta el punto de resultar insuficiente concebir la intimidad como un derecho de defensa frente a cualquier intromisión en la esfera privada, sin considerarla, simultáneamente, como un derecho activo de control sobre el flujo de informaciones que afectan a cada sujeto [92].

La protección jurídica de los datos personales constituye una de las más relevantes y actuales manifestaciones de los instrumentos de tutela de los derechos y libertades fundamentales. Su razón de ser estriba en el surgimiento de un fenómeno cualitativa y cuantitativamente nuevo, que se traduce siguiendo a Toniatti, en la posibilidad de tratamiento informático por parte de una multitud de operadores, de una multitud de datos personales referidos a una multitud de sujetos [93]. Su reconocimiento supone, por tanto, una exigencia ineludible para la correcta articulación de los sistemas democráticos. En la teoría jurídica y jurisprudencial se hace referencia con este término al conjunto de bienes o intereses que pueden verse afectados por la elaboración de informaciones referentes a personas identificadas o identificables [94]. Como señala Denninger, la protección de los datos personales forma parte del conjunto de derechos que definen el *status constituens* del ciudadano, su posición jurídica de formar parte activa y constituyente del Estado [95].

a. Algunas precisiones conceptuales.

Los problemas conceptuales planteados no se limitan al término intimidad, sino que alcanzan a otros con el conexos o vinculados. Tal es la situación del concepto "*protección de datos*". Cuando nos planteamos las posibles relaciones o interferencias entre informática y derecho, asoma, casi instintivamente, la noción de protección datos, y junto a ella toda un elenco de términos de aquel

[91] Cfr. CASCAJO CASTRO, J.L., "Tratamiento automatizado de los datos de carácter personal", en la obra colectiva, ed. a cargo de J.M. Sauca, *Problemas actuales de los derechos fundamentales*, Universidad Carlos III & Boletín Oficial del Estado, Madrid, 1994, p. 365; PEREZ LUÑO, A.E., "Dilemas actuales de la protección de la intimidad", *Ibid.*, p. 319.

[92] Cfr. PEREZ LUÑO, A.E., *Derechos humanos, Estado de Derecho y Constitución*, cit., p. 330; ID, "Dilemas actuales de la protección de la intimidad", cit., p. 318.

[93] Cfr, TONIATTI, R., "Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada", en *Revista Vasca de Administración Pública*, núm. 29, enero-abril 1991, p. 141.

[94] Cfr. PEREZ LUÑO, A.E., *Libertad informática y leyes de protección de datos*, cit., p. 139.

derivados, tales como "*datos personales*", "*tratamiento de datos*", "*fichero automatizado*", "*afectado*", etc...

Es por ello que, al igual que se ha realizado con la noción de intimidad, sea necesario proceder a una depuración y aclaración terminológica que nos permita determinar a que nos estamos refiriendo y cúal es el objeto que se pretende salvaguardar con tales medidas protectoras.

Señala Pérez Luño a este respecto, como el termino "*protección de datos*" hace referencia al *conjunto de bienes o intereses que pueden ser afectados por la elaboración de informaciones referentes a personas que pueden ser identificadas o identificables.* Denominación que se ha consolidado tras su incorporación a múltiples textos normativos [96].

Asi se hace referencia a la existencia de una serie de leyes de protección de datos que, siguiendo al precitado autor, tienen por objeto la protección de las personas respecto al tratamiento automatizado de datos de carácter personal y que, al igual que los derechos humanos, se han visto sometidas a un proceso de evolución generacional [97].

No obstante esta aclaración, se impone, como así han hecho la mayoría de las legislaciones nacionales e internacionales sobre la materia, la delimitación conceptual de los términos utilizados en los textos normativos, lo que presenta un indudable interés como contribución a precisar el nuevo vocabulario en el que se formulan lingüísticamente las relaciones entre informática y derecho. Se impone, en definitiva, lejos de quedar relegados a una concepción meramente descriptiva, la necesidad de operar con una serie de definiciones *explicativas*, que tiendan a individualizar algunos trazos que aclaren el sentido de la expresión genérica "protección de datos", para poder captar el sentido y alcance actual de esta expresión [98].

Así, de entre el numeroso elenco de definiciones incorporadas por los textos, si conviene desde este instante proceder a la depuración de aquellos que se revelan como fundamentales en nuestra reflexión y que constituirán los goznes conceptuales en torno a los cuales girará nuestro caminar.

[95] Cfr. DENNINGER, E., "El derecho a la autodeterminación informativa", trad. cast. de A.E. Pérez Luño, en la obra colectiva, edic. a cargo de A.E. Pérez Luño, *Problemas actuales de la documentación y la informática jurídica*, Tecnos, Madrid, 1987, p. 274.

[96] Cfr. PEREZ LUÑO, A.E., "Nuevos derechos fundamentales de la era tecnológica", cit., pp. 172-173. La negrita es nuestra.

[97] Cfr. PEREZ LUÑO, A.E., *Libertad informática y leyes de protección de datos*, cit., especialmente pp. 145-154.

[98] En torno a las nociones de definiciones *lexicales y explicativas*, vid., PEREZ LUÑO, A.E., *Derechos humanos, Estado de Derecho y Constitución*, cit., pp. 238-245.

Esas definiciones aluden a:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables [99]. Si la delimitación de qué sea persona física identificada no plantea problemas, si los acarrea el intento de conceptuación de "persona física identificable". Una poderosa ayuda nos la proporciona, desde el ámbito del Derecho Comunitario Europeo, la propuesta de Directiva relativa a la protección de datos personales cuando señala que se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social [100].

b) Tratamiento automatizado: cualquier operación o cualquier conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción [101].

c) Afectado: persona física titular de los datos que sean objeto de un tratamiento automatizado. Esta definición, auténtica innovación de la legislación española de protección de datos, y que no encuentra acomodo en otros texto similares del Derecho comparado, presenta además una serie de problemas que conviene en este momento dilucidar para evitar equivocos posteriores y de más hondo calado.

La referencia a una persona "titular" de los datos parece remitir a una especie de derecho propietario de los ciudadanos sobre sus datos. La protección de los datos personales correría, de asumirse esta visión, el riesgo de convertirse en un derecho de contenido patrimonial y se limitaría su eficacia práctica al someterlo a esa "optica privatista" [102]. Algún sector doctrinal propuso la comparación entre el derecho a la vida privada y el derecho de propiedad privada. Analogía sugestiva

[99] Definición recogida en el art. 2 del 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. En idéntico sentido se manifiesta en el ordenamiento jurídico español el punto a) del art. 3 de la Ley Orgánica 5/ 1992 de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD).

[100] Cfr. art. 2 a), de la Posición Común (CE) Nº 1/95, adoptada por el Consejo el 20 de febrero de 1995, con vistas a la adopción de la Directiva 95/../CE del Parlamento Europeo y del Consejo, de.., relativa a la protección de las personas físicas en lo que respecta al tratamiento automatizado de los datos personales y a la libre circulación de estos datos, DOCE Nº C 93/7, de 13.4.95.

[101] Cfr. art. 2 b) de la Posición Común..., cit. En el mismo sentido, aunque de una manera no tan comprensiva de todos sus aspectos, el punto c) del art. 3 de la LORTAD, y el art. 2 del Convenio 108 del Consejo de Europa.

[102] Cfr. PEREZ LUÑO, A.E., *Libertad informática y leyes de protección de datos*, cit., p. 156.

pero que, sin embargo, como señala Frosini, no puede establecerse por cuanto con la protección de datos personales, en referencia con la intimidad, no se alude a un derecho privado y de contenido patrimonial, sino más bien a la esfera de los derechos políticos ejercitados por los ciudadanos. Lejos de entenderse como libertad aristocrática, se perfila como libertad democrática que concerniente a todos, en las relaciones sociales que tomaron nuevas formas gracias a la civilización tecnológica [103].

Aclaradas y convenientemente reconducidas las dudas terminológicas y conceptuales que nos asaltaban, nos encontramos ya en disposición de proseguir nuestra andadura a la busqueda de cúal sea el lugar que en, el marco de las relaciones entre el Derecho y las nuevas tecnologías, corresponde a los derechos y libertades de los ciudadanos.

b. De la intimidad a la libertad.

La protección de los datos personales encuentra su *ratio*, no ya en la protección de ese ámbito íntimo de la vida personal que se desea ver preservado, sino en la posibilidad de control sobre ciertos datos que hablan de nosotros, que muestran a los demás como somos, actuamos y sentimos; es decir, en la necesidad de proteger al individuo frente al peligro que supone el acopio y la transmisión de datos y que pueden hacer del hombre un ser transparente.

La necesidad, por tanto, de proteger los datos personales frente a eventuales abusos informáticos, dentro del ámbito de las libertades de los ciudadanos, viene determinada por las exigencias propias de un Estado de Derecho, como protección, no sólo de la intimidad, sino también de los derechos y libertades públicas en sentido amplio, frente a los excesos y abusos que conllevaría un poder absoluto e incontrolado de la Administración y de otras entidades sobre esos datos, poniendo en peligro la propia identidad personal [104].

Para evitar estos riesgos y amenazas es preciso situar el estatuto de las libertades a la altura de los nuevos apremios [105]. Nótese que hablamos de libertad y no exclusivamente de intimidad. Ésta no es más que un aspecto parcial y concreto de aquélla, y así se manifiesta si consideramos que mediante la lesión de la intimidad, violando el derecho a mantener intacta la zona más reservada del ser humano, se ocasiona un ataque a la propia libertad. No debe olvidarse, como señala Boix Reig, que lo que se ve

[103] Cfr. FROSINI, V., "Banco de datos y tutela de la persona", en *Revista de Estudios Políticos*, núm. 30, noviembre-diciembre 1982, pp. 24-25.

[104] Cfr. TASENDE CALVO, J.J., "Notas al Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal", en *Poder Judicial*, núm. 23, septiembre 1991, p. 106.

[105] Cfr. PEREZ LUÑO, A.E., "La contaminación de las libertades en la sociedad informatizada...", cit., p. 288.

menoscabada es la libertad, que padece con la simple fiscalización de esa zona nuclear de la personalidad, o con la instrumentalización de la persona mediante el conocimiento adquirido por cualesquiera medios de su ámbito privado [106].

Por otro lado, conviene tener en cuenta que la protección de datos personales frente a la informática abarca no sólo los datos de carácter íntimo, sino también aquellos otros aparentemente inocuos y conocidos. Conocimiento, como ya señalamos anteriormente, necesario para la consecución y satisfacción de intereses individuales y colectivos. Consecuentemente, si los datos son conocidos, ya no cabe hablar de protección de algo íntimo, desconocido y ajeno por/a los demás. La preservación del carácter íntimo de los datos deja de ser el valor prevalente en la problemática de su protección, y se atiende ahora a la posibilidad de disposición sobre los mismos al margen de su carácter secreto o no.

Es decir, en la posibilidad de que el ciudadano controle sus propios datos personales; en el aseguramiento de un marco de libertad personal que le permita decidir sobre los datos identificativos de su personalidad. Como ha señalado Frosini, "en el marco de la sociedad tecnológica se presentan nuevas formas de libertad personal, que no es más la libertad negativa de prohibir o impedir la utilización de informaciones personales, sino la libertad positiva de ejercer un control sobre los datos concernientes a la propia persona, que hayan ya salido del ámbito de la esfera de la intimidad para convertirse en elementos de una base de datos automatizada" [107].

Esta libertad que venimos pregonando como referente articulador y central de la protección de los datos personales, no es más que una emanación del valor fundamental del libre desarrollo de la personalidad [108]. Valor, que siguiendo a Podlech, se divide en dos libertades básicas: la libertad general de acción, entendida como libertad para decidir la realización u omisión de determinados actos y la facultad consiguiente de comportarse o actuar de acuerdo con esa decisión, y la autodeterminación informativa, que se refiere a la libertad para determinar quién, qué y con qué ocasión pueden conocer informaciones que conciernen a cada sujeto [109].

[106] Cfr. BOIX REIG, J., " Protección jurídico-penal de la intimidad e informática", en *Poder Judicial*, núm. Especial IX, 1989, p. 19.

[107] Cfr. FROSINI, V., " Banco de datos y tutela de la persona", en *Revista de Estudios Políticos*, núm. 30, noviembre-diciembre 1992, p. 24.

[108] Cfr. PEREZ LUÑO, A.E., "Intimidad y protección de datos personales: del habeas corpus al habeas data", cit., 38.

[109] *ID.*, "Nuevos derechos fundamentales de la era tecnológica...", cit. p. 188. En evidente paralelismo, y partiendo del derecho a la intimidad, el denominado *Informe Younger sobre la intimidad* distingue dos facetas de este derecho: a) la intimidad "física" que supone "libertad frente a toda intromisión sobre uno mismo, su casa, su familia y sus relaciones" y la intimidad informativa que es "el derecho a determinar por uno mismo cómo y en qué medida se puede comunicar a otros información sobre uno mismo".

De todo lo expuesto puede extraerse como la concepción tradicional de la intimidad se revela sin duda insuficiente para hacer frente a los problemas derivados para los derechos y libertades de los ciudadanos por las nuevas tecnologías informáticas. Además también ha quedado acreditado como en el momento actual del desarrollo social la mayor parte de las actividades personales no están amparadas por la intimidad [110]. La interrelación entre informática y derechos fundamentales, no limita su campo de acción sólo al derecho a la intimidad. No todas las manifestaciones de la sociedad tecnológica y de la informática afectan a la intimidad; ni sus repercusiones sobre los derechos de los ciudadanos se refieren sólo y exclusivamente a la intimidad. Que duda cabe que el sector de la intimidad es uno de los más directamente afectados, pero no es el único.

La correcta articulación en la protección de los datos personales se resuelve no ya en un problema de intimidad, sino de libertad. Asistimos a un proceso más amplio, más global; en el que no sólo nos jugamos nuestra vida privada, sino nuestra propia identidad como seres humanos y ciudadanos.

La cuestión reside, por tanto, en determinar si ese derecho a la intimidad, aunque adaptado a las exigencias sociales e históricas, susceptible de ampliar su cobertura y de adaptarse a las nuevas necesidades, puede servir de soporte jurídico para la tutela jurídica de la persona frente a la informática, o si es preciso crear otro soporte para conseguir ese objetivo [111]. O, formulado de otro tenor, si las nuevas facetas de la intimidad propias de las sociedades tecnológicas precisan nuevos instrumentos de tutela jurídica [112]. Ante este dilema, la ciencia jurídica debe concretar este ámbito, ya sea desarrollando a partir de él nuevos derechos o introduciendo nuevos caracteres, nuevos garantías y nuevos límites que permitan hacer frente a estos nuevos medios, limitándolos y prohibiéndolos cuando se abuse de ellos [113].

3.3. *La delimitacion del derecho a la libertad informática.*

Planteábamos al final del punto precedente la alternativa entre la remoción de los viejos principios jurídicos de la intimidad, para adaptarlos a las nuevas exigencias de la sociedad tecnológica; o la necesidad de nuevos mecanismos de tutela jurídica para hacer frente a un problema nuevo. Alternativa que no es más que la consecuencia lógica de la visión histórica, generacional y abierta del catálogo de los derechos humanos que venimos sosteniendo a lo largo de nuestra exposición.

[110] Cfr. PEREZ LUÑO, A.E., "Informática Jurídica y Derecho de la informática en España", en *Informatica e Diritto*, núm. 2, 1983, p. 93.

[111] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., p. 99.

[112] Cfr. PEREZ LUÑO, A.E., "Dilemas actuales de la protección de la intimidad", cit., p. 316.

[113] Cfr. ROVIRA VIÑAS, A., "Reflexiones sobre el derecho a la intimidad en relación con la informática...", cit., p. 262.

Más que la intimidad en sentido estricto es la autodeterminación informativa, como señala Lucas Murillo de la Cueva, la que está en juego cuando se habla de los peligros de la informática. Como se ha puesto de manifiesto, su ámbito comprende más allá de lo que es la esfera privada [114], para identificarse en la defensa de la personalidad, de esa libertad necesaria para el libre desenvolvimiento de la persona en cuanto ser integral, con el bien a proteger. La voluntad de acentuar la dimensión subjetiva que reviste la protección de las personas frente a determinados usos de las tecnologías contribuyó, como ha señalado certeramente Pérez Luño, a la configuración de un nuevo derecho fundamental: La libertad informática o el derecho a la autodeterminación informativa [115].

La libertad informática, o autodeterminación informativa, se presenta así como la respuesta histórica de los Estados de Derecho más avanzados frente a las amenazas que dimanan para el disfrute de las libertades de distintos empleos de las nuevas tecnologías. Esos procesos tecnológicos engendran invasiones potenciales o reales en la intimidad y demás libertades; y, al propio tiempo, condicionan la capacidad de los ciudadanos para actuar libremente, para elegir sus formas de comunicación con su medio, y para participar en la vida social y política. La dialéctica nuevas necesidades/nuevos derechos se cumple, de este modo, plenamente en la génesis y fundamento de la libertad informática. [116]

Ahora bien, la formulación de este nuevo derecho no está exenta de una viva polémica en el campo doctrinal patrio y foráneo. Las discrepancias surgen desde el momento mismo de la elección de una denominación acorde con su objeto, se acrecientan en la determinación de su contenido y se hacen manifiestamente beligerantes cuando se trata de determinar su carácter autónomo o su dependencia respecto de derechos o valores formulados con anterioridad.

3.3.1. Delimitación conceptual: El derecho a la libertad informática y otros conceptos y categorías afines.

Observará el lector como venimos usando los términos de "libertad informática", "autodeterminación informativa" y "protección de datos". Junto a ellos han aparecido otros como "identidad informática", "intimidad informática" o "intimidad informativa".

[114] Cfr. LUCAS MURILLO DE LA CUEVA, P., "La protección de los datos personales ante el uso de la informática", en *Anuario de Derecho Público y Estudios Políticos*, núm. 2, 1989/90, p. 158; *ID, El derecho a la autodeterminación informativa*, cit., p. 120.

[115] Cfr. PEREZ LUÑO, A.E., y de entre su numerosa producción científica sobre este aspecto: *Libertad informática y leyes de protección de datos*, cit., p 139-140; "Nuevos derechos fundamentales de la era tecnológica...", cit., pp. 187-ss; "Intimidad y protección de datos personales...", cit., p. 40; "Dilemas actuales de la protección de la intimidad", cit., p. 316.

[116] Cfr. PEREZ LUÑO, A.E., " Nuevos Derechos fundamentales de la era tecnológica...", cit., p. 192.; *ID, Libertad informática y leyes de protección de datos*, cit., p. 160.

Tal proliferación de denominaciones no hace sino encubrir las diferentes concepciones que acerca de este derecho se tienen en la doctrina, y que no es más que el campo de batalla en el que se dilucida cual es el verdadero papel que corresponde a este nuevo derecho en la defensa de los valores e intereses ciudadanos. De ahí que sea necesario abordar su estudio desde una perspectiva global, que acoja todos los aspectos problemáticos y su posible resolución.

Múltiples han sido las definiciones que de este derechos se han elaborado. Sin ánimo de ser exhaustivos, si que conviene tener en cuenta las más relevantes, por cuanto pueden aportarnos elementos para la determinación de su contenido y su naturaleza jurídica.

Para Pérez Luño, en una definición que se ha convertido en referente inexcusable para la comprensión de este nuevo derecho, la libertad informática comporta garantizar a las personas el derecho fundamental a: a) la *información*, esto es, la posibilidad de conocer los bancos de datos existentes, así como su titularidad y finalidad; b) el *control* que se desglosa, a su vez, en la facultad de acceso por parte de los afectados a las informaciones que les conciernen, en lo que se ha visto la consagración de un *habeas data* por su finalidad equiparable al clásico *habeas corpus*, la facultad de *corrección* de los datos inexactos o procesados indebidamente, el denominado derecho al *olvido*, esto es, el principio a tenor del cual ciertas informaciones deben ser eliminadas de los *dossiers* transcurrido un determinado período de tiempo desde el momento en que acaeció el hecho a que se refieren para evitar que el individuo quede prisionero de su pasado; y c) la *tutela* de las facultades anteriores mediante el establecimiento de los oportunos recursos [117].

Frosini la conceptúa como el derecho de autotutela de la propia identidad informática: o sea el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en las tarjetas de un programa electrónico [118]. O como el mismo autor ha establecido, con una mejor determinación de los atributos que lo componen, la libertad informática consistiría en el derecho a poder disponer de los datos de información personal propios y, por tanto, a permitir o rehusar su uso por parte de las agencias de información que manejan los bancos de datos; derecho a controlar la veracidad de los datos, el acceso a su conocimiento por parte de terceros, el uso que de ellos se hiciere con finalidades sociales, económicas, políticas.

Para Lucas Murillo de la Cueva consistiría en el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente

[117] Cfr. PEREZ LUÑO, A.E., "Informática jurídica y derecho de la informática en España", cit., pp. 93-94. Definición asumida en sus trabajos posteriores: *Nuevas tecnologías, sociedad y derecho*, cit., p. 85-ss; *ID, Libertad informática y leyes de protección de datos*, cit., p. 140; *ID*, "Nuevos derechos fundamentales de la era tecnológica...", cit., p. 173.

[118] Cfr, FROSINI, V., "Bancos de datos y tutela de la persona", cit., p. 24.

sea íntima o no para preservar, de este modo y en último extremo, la propia identidad, nuestra dignidad y libertad [119].

Alvarez-Cienfuegos, en una aproximación mas generalista, considera como tal la facultad de elección de la persona sobre la revelación o no de informaciones que directamente le conciernen [120].

Denninger, por último, y siguiendo lo establecido por el Bundesverfassungsgerichts en su Sentencia de 15 de diciembre de 1983 sobre la Ley del Censo de Población [121], entiende que el derecho a la autodeterminación informativa consiste en la competencia de cada individuo "de disponer principalmente sobre la revelación y el uso de sus datos personales" [122].

Nótese como algunas de las conceptuaciones apuntadas incorporan un nuevo término: "identidad" o "identidad informática"; que no debe considerarse contrapuesto al de libertad informática, sino parte integrante del mismo. La "identidad informática" haría referencia, de esta forma, al conjunto de datos personales que debidamente aunados y/o entrecruzados arrojarían como precipitado un perfil de nuestra personalidad, una radiografía de como somos y actuamos. La posibilidad de accionar contra esa posibilidad de determinar el estatuto personal sólo por el simple acopio o entrecruzamiento de datos personales constituye en última instancia el objetivo a satisfacer con este nuevo derecho.

Esta aclaración que puede resultar baladí u obvia, no lo es tanto, cuando nos encontramos en la doctrina patria con intentos definitorios que, lejos de aclarar el tema objeto de debate, tienden a complicarlo más, por la confusión terminológica y conceptual en que incurren. Sirva como ejemplo paradigmático de esta desorientación conceptual lo señalado por Romeo Casabona, cuando indica: " En la actualidad, la tendencia de la protección de la intimidad personal frente a la informática parte del principio siguiente: garantizar la libertad informática; esto significa que no se trata tanto del derecho del Estado al conocimiento y al uso de los datos informáticos referentes a los ciudadanos, como del derecho de éstos a conocer lo relativo a sus propios datos, a tener acceso a los mismos para lograr la llamada *identidad informática* y controlar la utilización que se vaya a dar a esos datos. Para lograr esa identidad y, en un último extremo, intimidad informáticas, se derivan en concreto de este derecho...." [123]. Queda patente la confusión terminológica: la

[119] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales* (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal), Centro de Estudios Constitucionales, Madrid, 1993, p. 33.

[120] Cfr. ALVAREZ-CIENFUEGOS SUAREZ, J.M., "El derecho a la intimidad personal, la libre difusión de la información y el control del Estado sobre los Bancos de Datos", en *Actualidad Administrativa*, núm. 37, 1991, p. 464.

[121] La Sentencia se ha publicado en trad. cast. de M. Daranas, por la que se cita, en *BJC*, núm. 33, 1984, pp. 126-170.

[122] Cfr. DENNINGER, E., "El derecho a la autodeterminación informativa", cit., p. 273.

[123] Cfr. ROMEO CASABONA, C.M., *Poder informático y seguridad jurídica*, cit., p, 32.

identidad informática se equipara con el derecho de acceso, obviando todos los procesos de tratamiento de datos, que es precisamente donde esa identidad puede verse menoscabada; se utilizan los términos "libertad informática" e "intimidad informática" como aparentemente sinónimos, incurriendo en una dualidad terminológica si lo que se pretende es definir la misma realidad; se confunde formulación de un derecho con las facultades que son inherentes a su contenido, etc... Pese a lo defectuoso de este planteamiento tiene la cualidad positiva de un esfuerzo intelectual; otros simplemente asumen postulados y aportaciones elaborados con anterioridad, dándoles, en algunos casos, el carácter de propios.

Por otra parte, los términos "libertad informática" y "protección de datos" parecen ser los que gozan de mayor predicamento en la doctrina. Junto a él cobra fuerza el de "derecho a la autodeterminación informativa", formula paralela a la libertad informática elaborada por la doctrina y jurisprudencia alemanas.

La dualidad terminológica - libertad informática vs. autodeterminación informativa - ha dado pie a la impugnación de la equivalencia y condicionamiento mutuo de ambos términos; haciéndolos aparecer como contrapuestos y afectantes a diferentes ámbitos.

Sin embargo, como ha señalado Pérez Luño, la libertad informática y el derecho a la autodeterminación informativa pueden considerarse, por tanto, como sinónimos; en cuanto se concreta en la garantía de acceso y control de las informaciones por parte de las personas concernidas [124].

De igual modo, la dualidad terminológica representada por la protección de datos y la libertad informática, se resuelve en que ambas categorías se condicionan mutuamente y representan, siguiendo a Pérez Luño, los dos aspectos de una misma moneda, en este caso, de un derecho fundamental. La protección de datos en cuanto supone un ordenamiento objetivo de las bases de datos, esto es, implica un conjunto de decisiones básicas sobre su estructura y funcionamiento tendente a garantizar el equilibrio de poderes en las sociedades democráticas. La libertad informática en lo que entraña de proyección de ese orden informático a la esfera de las situaciones subjetivas. En síntesis: la protección de datos carecería de sentido sino se tradujera en un conjunto de garantías para las personas; pero, al propio tiempo, la libertad informática o el derecho a la autodeterminación informativa serían inconcebibles de no contar como presupuesto una opción axiológica *sobre* y un marco organizativo *de* la información [125].

Establecida la pertinente depuración terminológica, la pequeña muestra esbozada de las principales aportaciones conceptuales pone de manifiesto que, al mar-

[124] Cfr. PEREZ LUÑO, A.E., *Libertad informática y leyes de protección de datos*, cit., p. 141; ID, "Intimidad y protección de datos personales", cit., p. 39.

[125] Cfr. PEREZ LUÑO, A.E., "Nuevos derechos fundamentales de la era tecnológica", cit., p. 175; *ID, Libertad informática y leyes de protección de datos*, cit., p. 141.

gen de diferentes denominaciones, la mayor parte de la doctrina autorizada se halla de acuerdo en torno al contenido esencial de la libertad informática o derecho a la autodeterminación informativa.

El contenido típico del derecho a la libertad informática estaría así integrado por diferentes facultades y poderes de control que se reconocen a sus titulares sobre la información personal que les afecte así como por los deberes y obligaciones que recaen sobre los sujetos pasivos y por las reglas objetivas, procedimientos e instituciones de garantía predispuestos por el legislador [126], que abarca todas las fases de elaboración y uso de los datos, o sea, su acumulación, su transmisión, su modificación y su cancelación [127].

3.3.2. La determinación de su naturaleza jurídica. La afirmación de su autonomía.

Si las diferencias terminológicas son más o menos reconducibles a un punto de encuentro, donde no existe una posibilidad de consenso es cuando se pretende hacer frente a la cuestión de cúal sea la naturaleza jurídica del derecho a la libertad informática. Es decir, si nos hallamos ante la reformulación de consolidados valores jurídicos; o más bien, asistimos al nacimiento de un nueva categoría jurídica, de un nuevo derecho fundamental.

La primera opción ha sido acogida entre quienes consideran la libertad informática como una manifestación de la intimidad en la sociedad informatizada, emanación a su vez de un genérico, y limitado en sus manifestaciones, derecho al libre desarrollo de la personalidad. Así Toniatti, al plantearse las posibles interacciones entre informática e intimidad, señala como necesaria la búsqueda de un equilibrio entre la protección de las informaciones y la garantía de otros valores jurídicos, *inscribibles en la noción de intimidad,* considerados merecedores de tutela [128]. Señalando con posterioridad, y de una manera más contundente, como, incluso frente a la expresa consideración del derecho al libre desarrollo de la personalidad como su fundamento textual, parece preferible considerar que "el derecho a la autodeterminación informativa" es un nuevo *nomen iuris* de un derecho ya conocido más que un autónomo y diverso derecho fundamental de creación jurisprudencial [129].

Por su parte, en la doctrina española, mayoritariamente afecta a estas tesis, Madrid Conesa, se decanta por esta vía cuando tras señalar la realidad del fenómeno informático y de la existencia de los bancos de datos, pone de manifiesto la necesi-

[126] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., p. 117; *ID, Informática y protección de datos personales*, cit., p. 55.
[127] Cfr. PEREZ LUÑO, A.E., "Nuevos derechos fundamentales de la era tecnológica", cit., p. 174.
[128] Cfr. TONIATTI, R., "Libertad informática y derecho a la protección de datos personales", cit., p. 142.
[129] *Ibidem*, p. 162.

dad de hacer frente a los peligros que se derivan para el derecho a la intimidad. Si bien posteriormente parece matizar esta postura cuando, al analizar lo señalado por el art. 18.4 de nuestro texto constitucional, constata como la protección dispensada por tal precepto no sólo se limita al derecho a la intimidad, sino a todos los derechos "ante la dificultad de determinar todos los bienes jurídicos afectados" [130].

En el mismo sentido se manifiesta Boix Reig al indicar que "el uso informático del tratamiento automatizado de los datos personales debe limitarse por las propias exigencias de un Estado de Derecho, en el que constituye esencial la intimidad como elemento integrador y configurador de la personalidad" [131].

La doctrina alemana, más partidaria de ampliar los valores constitucionales ya reconocidos, como el libre desarrollo de la personalidad, que de aumentar el catálogo de los derechos fundamentales con derechos no reconocidos expresamente en la Grundgesetz, se ha decantado mayoritariamente por esta opción.

Simitis entiende, al considerar la sentencia del Bundesverfassungsgerichts sobre la Ley del Censo de población, que aunque la sentencia no ha supuesto propiamente el nacimiento de un nuevo derecho fundamental y, en concreto, de un derecho fundamental a la protección de datos entendido como una categoría independiente y autónoma, constituye un precedente de decisiva importancia para la delimitación de las condiciones básicas para el tratamiento automatizado de datos e informaciones conforme a la Constitución [132].

Pese a lo variado de la argumentación esgrimida, las diferentes aportaciones señaladas coinciden en señalar la dependencia de la libertad informática o autodeterminación informativa , bien del concepto más restringido de intimidad; o bien del más amplio de libre desarrollo de la personalidad. Y aunque tal derivación no es del todo incorrecta, si lo es el negar la posibilidad de evolución axiológica y su consolidación en nuevas formas de tutela jurídica a través de la formulación de nuevos derechos fundamentales. La intimidad o el libre desarrollo de la personalidad no constituyen el objeto a proteger; son el punto de partida que nos introduce en una nueva dimensión, en una problemática desconocida hasta la hora presente, y cuya resolución, por ese carácter *ex novo*, requiere de nuevos instrumentos de tutela. Aparece de nuevo, cual fantasma, esa temerosa visión inmovilista del catálogo de los derechos humanos a la que reiteradamente nos hemos referido.

Frente a estas tesis reduccionistas, se han alzado voces reclamando la necesaria e inexcusable consolidación de nuevas garantías jurídicas para hacer frente a

[130] Cfr. MADRID CONESA, F., *Derecho a al intimidad, informática y Estado de Derecho,* cit., pp. 36-ss.
[131] Cfr. BOIX REIG, J., "Protección penal de la intimidad e informática", cit., p. 25.
[132] Cfr. PEREZ LUÑO, A.E., " La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo", cit., pp. 260 - 264.

los retos planteados por el tratamiento automatizado de los datos personales y su incidencia en la vida de los ciudadanos.

Así, como hace Frosini, se aboga por el reconocimiento de una nuevo derecho de libertad de las personas, que puede definirse como "derecho a la libertad informática"[133]; abogando por una afirmación de la libertad informática como principio unitario y universal de la sociedad tecnológica[134].

Denninger, partiendo de que el concepto de autodeterminación informativa halla su precedente en planteamientos doctrinales y jurisprudenciales previos, si reconoce que la sentencia sobre la Ley del Censo de Población ha supuesto una contribución muy valiosa para las garantía jurisdiccional de la protección de los datos personales, así como para la concreción del derecho a la autodeterminación informativa, entendido como el presupuesto para el funcionamiento de los sistemas informatizados de tratamiento de datos en un Estado de Derecho inspirado en los principios de libertad y democracia [135].

Ha sido la doctrina española, sin embargo, la que de una manera más depurada ha contribuido a poner de manifiesto el carácter autónomo de este nuevo derecho y la necesidad de afirmación de sus rasgos diferenciadores con derechos o valores formulados con anterioridad.

Sin poder detenernos en todas las aportaciones de la doctrina patria, tomaremos como consideraciones emblemáticas aquellas que, a nuestro modesto criterio, gozan de una mayor depuración científica.

Lucas Murillo de la Cueva aboga por ese reconocimiento de un nuevo derecho fundamental, cuando partiendo de una argumentación comprensiva de todos los aspectos conflictivos, señala de una manera sintética, pero didáctica que " el bien que tutelan los sistemas de protección de datos no es la intimidad "física" o entendida en sentido estricto, sino la... autodeterminación informativa, cuya diferencia respecto a las primeras hemos intentado poner de manifiesto... Si, además, estamos en presencia de una disciplina jurídica específica que cada vez se amplia más y se caracteriza por el régimen singular que establece; si, por otra parte, existen ya nuevas categorías conceptuales y una sistematización teórica que encuadra, en su lugar propio, todo este sector no vemos razones que impidan hablar de un nuevo derecho: el derecho a la autodeterminación informativa"[136].

[133] Cfr. FROSINI, V., "Los derechos humanos en la sociedad tecnológica", cit., p. 113.
[134] Cfr. FROSINI, V., "Bancos de datos y tutela de las personas", cit., p. 40.
[135] Cfr. DENNINGER, E., "El derecho a la autodeterminación informativa", cit., p. 274.
[136] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., pp. 123-124, y la amplia bibliografía, referente a la doctrina española, allí citada. Esta tesis ha sido acogida y reiterada en su trabajo posterior, *Informática y protección de datos personales*, cit., p. 31.

Pero ha sido, sin ninguna duda, la aportación de Pérez Luño la que presenta un carácter más completo, más depurado y la que más amplio eco ha tenido en la discusión acerca del *status* de este nuevo derecho. Tras mostrar su discrepancia con la consideración de la libertad informática como apéndice de otros valores o derechos básicos, reivindica, por tanto, la conceptuación de la libertad informática como derecho fundamental, apoyándose en los siguientes argumentos:

"a. Las reservas a reconocer la autonomía de este nuevo derecho residen en su vinculación con una concepción de la intimidad en sentido individual, circunscrita a garantizar al individuo una esfera de soledad y aislamiento.

Actualmente el centro de atención se ha trasladado desde la consideración de la intimidad como facultad de aislamiento al poder de control sobre las informaciones que son relevantes para cada sujeto. Precisamente esa facultad de elección de la persona acerca de la revelación o no de sus datos personales, constituye el núcleo de la libertad informática, en cuanto aspecto básico de la intimidad.

b. La negación de la autonomía de este derecho, para englobarlo en el marco general del derecho al libre desarrollo de la personalidad, entorpecería gravemente la relación del derecho a la libertad informática con otros derechos.

Las concordancias que se establezcan no serían posibles sino se reconoce a la libertad informática como un derecho fundamental autónomo. Si se concibe al *habeas data* y las restantes facultades que configuran la libertad informática como un mero apéndice de otros valores, no podrá propugnarse sino una conexión indirecta con otros valores y derechos a través de esos otros valores que, en su caso, deberán servirle de soporte.

No obstante, las reservas expuestas por la doctrina a la autonomía de este nuevo derecho, puede afirmarse que la libertad informática permite una lectura renovada del conjunto de valores y derechos que fundamentales de aquellos sistemas constitucionales que la admiten.

c. Aquellas posiciones que impugnan la autonomía de la libertad informática, no son más que aquellas que cuestionan el carácter dinámico de los derechos fundamentales, y los conceptúan como un catálogo cerrado y completo.

Olvidan, por tanto, que una sociedad libre y democrática deberá mostrarse siempre abierta y sensible a la aparición de nuevas formas de agresión a la libertad y de nuevas necesidades, que fundamentan derechos nuevos.

d. La garantía de la protección de la libertad informática sólo podrá consolidarse si la concebimos como un derecho autónomo dotado de medios específicos de tutela. Por contra, si la consideramos disuelta en el ámbito de otros valores o derechos, la libertad informática corre el riesgo de relativizarse y ver comprometida su efectiva realización" [137].

[137] Cfr. PEREZ LUÑO, A.E., "Nuevos Derechos Fundamentales de la era tecnológica: la libertad informática ", cit., pp. 187-193; *ID, Libertad informática y leyes de protección de datos*, cit. pp. 157-151.

4. LA POSITIVACION DEL DERECHO A LA LIBERTAD INFORMÁTICA. LA CONSOLIDACION JURISPRUDENCIAL Y LEGISLATIVA.

El reconocimiento del derecho a la libertad informática como una nueva incorporación al catálogo, siempre abierto y en continua evolución, de los derechos fundamentales, no sólo hunde sus raíces en el esfuerzo intelectual de un sector doctrinal preocupado por establecer las relaciones del hombre con el complejo mundo tecnológico en que desarrolla su existencia. Además, y sobre la base de aquellas premonitorias reflexiones, se procedió a su positivación a través de una labor, primero jurisprudencial y después normativa, que tenía como objetivo último propiciar el reconocimiento y aplicación efectivos de este derecho. Es decir, establecidas las bases teóricas de un nuevo mecanismo de tutela jurídica, debía llevarse a la práctica para que los ciudadanos pudieran usar de él y proteger así sus libertades y derechos más preciados.

No siendo posible hacernos eco de todas la manifestaciones jurisprudenciales y legislativas sobre esta materia, nos detendremos en aquellas que por su carácter pionero y/o por lo relevante de sus aportaciones han contribuido a delimitar el status de este derecho, constituyendo, a la vez, la base de ulteriores reflexiones y planteamientos. Pero no todo, como veremos, será positivo, nos encontramos en un camino con múltiples recovecos, trampas y callejones sin salida. En ocasiones, cuando creemos avanzar, no estamos sino retrocediendo.

4.1. *La aportacion jurisprudencial.*

4.1.1. La Sentencia del Tribunal Constitucional Alemán sobre la Ley del Censo de Población.

En la configuración jurídica del derecho a la libertad informática ha jugado un papel pionero y relevante las Sentencia del Tribunal Constitucional Federal (Bundesverfassungsgericht) de la República Federal de Alemania de 15 de diciembre de 1983, en que se declara parcialmente inconstitucional la Ley del Censo de Población de 4 de marzo de 1982 [138].

[138] Para un estudio de la relevancia de la Sentencia en la doctrina germana, vid., entre otros: DÄUBLER, W., "Nuevas tecnologías-Nuevo Derecho. Reflexiones básicas en la experiencia laboral alemana", trad. cast. de A. Ojeda Avilés, en la obra colectiva, ed. a cargo de A.E. Pérez Luño, *Problemas actuales de la documentación y la informática jurídica* (Actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986), Tecnos & Fundación Cultural Enrique Luño Peña, Madrid, 1987, pp. 253-267; DENNINGER, E., "El derecho a la autodeterminación informativa", *Ibíd.*, pp. 269-276; SIMITIS, S., "Crisis de la información en el Derecho y sistemas informatizados de documentación jurídica", *Ibíd.*, pp. 53-59. En la doctrina española, vid. por todos: PEREZ LUÑO, A.E., "La defensa del ciudadano y la protección de datos", en *Revista Vasca de Administración Pública*, núm. 14, 1986, p. 44.

La ley de 1983 imponía a todos los habitantes la obligación de responder a un cuestionario sobre una serie de hechos de naturaleza personal, destinados, por un parte, a diversas administraciones y, por otra, a fines estadísticos.

El mérito de la sentencia de 15 de diciembre de 1983 reside en haber configurado el derecho a la intimidad como expresión de un derecho a la autodeterminación informativa. La jurisdicción constitucional ha deducido del derecho general de la personalidad uno de sus atributos: " la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida" [139]. Por ello, el Tribunal entiende "que no sería compatible con el derecho a la autodeterminación informativa un orden social y un orden jurídico que hiciese posible al primero, en el que el ciudadano ya no pudiera saber quién, qué, cuando y con qué motivo sabe algo sobre él... Ello no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, por que la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos." [140].

De todo ello extrae lo que puede considerarse la síntesis de su labor delimitadora, y así procede a señalar como "la libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitadas de los datos concernientes a la persona... garantiza, en efecto, la facultad del individuo de decidir básicamente por sí solo sobre la difusión y utilización de sus datos personales"[141].

Ahora bien, este derecho no presenta un carácter ilimitado. "El individuo no tiene ningún derecho sobre "sus" datos en el sentido de una soberanía absoluta e irrestringible, sino que es más bien una personalidad que se desenvuelve dentro de la comunidad social y que está llamada a comunicarse. La información, incluso en la medida en que se refiera a la persona como tal, ofrece un retrato de la realidad social que no cabe asignar exclusivamente al interesado... El individuo tiene, pues, que aceptar en principio determinadas limitaciones de su derecho a la autodeterminación informativa en aras del interés preponderante de la colectividad" [142].

Si bien dichas limitaciones han de ser aceptadas, las mismas, están sujetas a determinados requisitos que pueden sintetizarse en los siguientes:

— un fundamento legal (constitucional), del que se deduzcan con suficiente claridad y de modo inteligible para el ciudadano los supuestos y el ámbito

[139] La Sentencia se ha publicado, en trad. cast., de M. Daranas, por la que se citará, en BJC, 1984, núm. 33, pp. 126-ss; el texto reseñado se halla en la p. 152.
[140] Sentencia sobre la Ley del Censo, cit., p. 153.
[141] *Ibíd.*.
[142] *Ibíd.*, pp. 153-154.

de las limitaciones y que responda, por lo tanto, al imperativo de claridad normativa inherente al Estado de Derecho;
— un escrupuloso respeto al principio de proporcionalidad en la restricción de estos derechos fundamentales; es decir, que la medida sea adecuada y, además, indispensable para la consecución de los respectivos fines y la interferencia que lleve aparejada no puede, en cuanto a intensidad, ser desproporcionada a la importancia del objeto y a las cargas que imponga al ciudadano [143];
— adecuación de las medios a la finalidad perseguida por los procesos de documentación e información [144];
— garantías organizativas que eviten la posterior interconexión indebida de los datos, pues como el propio Tribunal señala los nuevos avances técnicos hacen que no haya hoy ningún dato sin interés [145].

No obstante, la interrogante acerca de la licitud de las restricciones del derecho a la autodeterminación informativa, sólo podrá hallar respuesta cuando se aclare, con carácter previo, la finalidad con la cual se recogen los datos y las posibilidades de su interconexión y utilización [146].

Por todo ello conviene el Tribunal en la necesidad de distinguir entre los datos relativos a la persona, susceptibles de recogida y elaboración en forma individualizada, no anónima, y los que destinen a fines estadísticos [147].

Por último, unos de los principios más interesantes extraídosde la Sentencia estriba en la aplicación al "poder informático" del principio constitucional de la separación o del equilibrio de poderes. Siguiendo a Rigaux, puede observarse en tres niveles: 1) en lo tocante a los datos de carácter personal, el respeto de la finalidad propia a cada categoría de datos prohíbe las interconexiones de varios ficheros automatizados, para evitar la derivación hacia otros usos de los datos recogidos para una finalidad precisa; 2) asimismo es preciso que las informaciones recogidas con fines administrativos sean rigurosamente separadas de las que tengan por objeto un tratamiento estadístico; 3) la vigilancia de los diversos tratamientos automatizados debe confiarse a una autoridad independiente, frente a la cual las autoridades administrativas y los responsables privados de ficheros automatizados no pueden prevalerse de ningún derecho al secreto [148].

[143] Cfr. TORNE-DOMBIDAU JIMENEZ, J., y CASTILLO BLANCO, F.A., " Informática y protección de la privacidad del individuo (II)", en Actualidad Administrativa, núm. 22, 7-13 junio 1993, p. 281.
[144] Cfr. PEREZ LUÑO, A.E., "La defensa del ciudadano y la protección de datos", cit., p. 46.
[145] *Ibíd.*
[146] Sentencia Ley del Censo.., cit., p. 154.
[147] Esta diferenciación se basa en la distinción radical operada por esta misma jurisdicción entre "datos de carácter personal", cuyo tratamiento permite la identificación de la persona física a la cual los datos se refieren y aplican, y los tratamientos que respetan el anonimato de los datos recogidos. Para un estudio profundo y exhaustivo de los planteamientos del Tribunal Constitucional alemán acerca del tratamiento automatizado de datos personales con fines estadísticos, vid. RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité,* Bruylant & L.D.G.J., Bruselas, 1990, pp. 588-592.

4.1.2. El Tribunal Europeo de Derechos Humanos. Las Sentencias Klass y Leander.

En el ámbito del Consejo de Europa, el Tribunal Europeo de Derechos Humanos (TEDH) ha desarrollado una importante labor en orden a la delimitación del derecho a la intimidad frente a las nuevas tecnologías [149]. Si bien sus primeras sentencias no hacen referencia expresa a la cuestión de la protección de datos, si incorporan importantes precisiones acerca de las posibles intromisiones en la vida privada de los ciudadanos por parte de las autoridades públicas y las garantías a que tal acto intromisorio debe estar sometido.

En este sentido, la Sentencia de 6 de septiembre de 1978, Caso KLASS y otros, constituye el punto de arranque en la configuración de esta línea jurisprudencial [150].

El origen de este pronunciamiento lo constituye el recurso formulado por Gerhard Klass y otros cuatro ciudadanos alemanes contra la Ley de 13 de agosto de 1968, que posibilita una restricción de las telecomunicaciones, correspondencia y envíos postales (la denominada Ley G 10). La cuestión a dilucidar era si tal restricción era compatible con lo establecido por el art. 8 del CEDH [151]. El Tribunal comienza señalando que aunque el punto 1. del art. 8 "no menciona las conversaciones telefónicas... ellas se encuentran comprendidas en las nociones de vida privada y de correspondencia señaladas por el texto" [152]. No siendo dudoso que la vigilancia secreta prevista por la legislación alemana implica una injerencia en el ejercicio del derecho enunciado en el art. 8.1, la cuestión a determinar es si tal injerencia está justificada en virtud del punto 2. del mismo artículo.

Para contestar a esta cuestión, el Tribunal distingue dos elementos. De una parte el objetivo perseguido por la G 10 entra dentro de los objetivos enumerados por el art. 8, punto 2, y a este respecto señala como "una apreciación en la extensión de la salvaguarda ofrecida por el art. 8, el Tribunal no puede constatar más que dos hechos importantes: los progresos técnicos realizados en materia de espionaje y paralelamente de vigilancia; en segundo lugar, el desarrollo del terroris-

[148] Cfr. RIGAUX, F., *La protection de la vie privée...,* cit., pp. 591-592.
[149] Para una correcta apreciación de la relevancia del Convenio Europeo de Derechos Humanos y de la jurisprudencia del TEDH, vid. CARRILLO SALCEDO, J.A., y de entre su numerosa producción científica: "El Convenio Europeo de Derechos Humanos", en *Actualidad Jurídica*, vol. 9, 1981, pp. 74-87; "El sistema jurisdiccional europeo de protección de los Derechos Humanos: La Comisión y el Tribunal Europeo de Derechos Humanos", en *Poder Judicial*, núm. Especial I, 1988, pp. 23-33; "Protección de derechos humanos en el Consejo de Europa: Hacia la superación de la dualidad entre derechos civiles y políticos y derechos económicos, sociales y culturales", en *Revista de Instituciones Europeas*, vol. 18, núm. 2, 1991, pp. 431-451.

mo en Europa en el curso de los últimos años. Las sociedades democráticas se encuentran amenazadas en nuestros días por formas muy complejas de espionaje y por el terrorismo, de suerte que el Estado debe ser capaz, para combatir eficazmente estas amenazas, de vigilar en secreto las elementos subversivos que operan en su territorio. El Tribunal debe, pues, admitir que la existencia de disposiciones legislativas acordando los poderes de vigilancia secreta de la correspondencia, de los envíos postales y de las telecomunicaciones son, ante una situación excepcional, necesarias en una sociedad democrática para la seguridad nacional y/o la defensa del orden y en la prevención de infracciones penales" [153].

Por otra parte, es necesario verificar si los medios empleados "quedan a este respecto dentro de los límites que son necesarios en una sociedad democrática". Reconociendo al legislador nacional "un cierto poder discrecional" en la elección de las modalidades de vigilancia, el Tribunal estima que le corresponde verificar la existencia de garantías adecuadas y suficientes contra los abusos. Ahora bien, tal poder discrecional no significa que los Estados nacionales dispongan de una discreción ilimitada para controlar con las medidas de vigilancia secreta a las personas sometidas a su jurisdicción. "Consciente del peligro de ver destruir la democracia con el motivo de defenderla, afirma que no sabrían tomar, en nombre de la lucha contra el espionaje y el terrorismo, no importa que medidas juzgadas por ellos apropiadas" [154].

Por ello, la vigilancia secreta debe verificarse en diferentes niveles. Si el carácter secreto de la vigilancia impide al interesado tomar parte directa en el control de tal actividad, se revela imprescindible que los procedimientos existentes proporcionen en sí las garantías apropiadas y equivalentes para la salvaguarda de los derechos del individuo. Se impone consecuentemente el respeto de los valores de una sociedad democrática, entre los que figura la preeminencia del Derecho. Ello implica que una injerencia del ejecutivo en los derechos de los ciudadanos debe verse sometida siempre a un control eficaz [155].

[150] Corte Europea de Derechos Humanos, caso Klass y otros, sentencia de 6 de septiembre de 1978, serie A, núm. 28; recogida, y en trad. cast. de A.J. Martínez Higueras, por la que se citará, en BJC. *Tribunal Europeo de Derechos Humanos 1959-1983*, Secretaría General del Congreso de los Diputados, Madrid, 1984, pp. 470-485.

[151] El art. 8 del CEDH establece:

" 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 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."

[152] Sentencia caso Klass, cit., p. 479.

[153] *Ibíd.*, p. 480.

[154] *Ibíd.*, cit., p. 480.

[155] *Ibíd.*, p. 481.

Para concluir sus alegaciones sobre la cuestión objeto de debate, el Tribunal considera como inherente al sistema del Convenio una cierta forma de conciliación entre los imperativos de defensa de la sociedad democrática y aquellos otros de la salvaguarda de los derechos individuales. Así como declara el Preámbulo del Convenio "el mantenimiento (de las libertades fundamentales) se apoya esencialmente sobre un régimen político verdaderamente democrático, de una parte, y, de otra parte, sobre una concepción común y un común respeto de los derechos del hombre". De acuerdo a lo prescrito en el art. 8 "esto significa que hay que buscar un equilibrio entre el ejercicio por el individuo del derecho (a la intimidad) y la necesidad de imponer una vigilancia secreta para proteger la sociedad democrática en su conjunto" [156].

La línea jurisprudencial abierta por esta sentencia ha sido de una importancia capital. Sus pronunciamientos, aún vigentes en la más moderna jurisprudencia, han posibilitado una visión amplia y realista de los derechos consagrados en el Convenio de 1950.

Así, y con base nuevamente en la posible infracción del art. 8 CEDH, el TEDH se ha pronunciado en el Caso Leander sobre la cuestión de la protección de los datos personales [157].

La sentencia, de 26 de marzo de 1987, tenía como origen la solicitud del señor Leander al no haber podido ocupar un puesto de trabajo debido a la existencia de una serie de antecedentes policiales y políticos en el Registro de la Policía. Estos datos hicieron que se le catalogara como "peligroso para la seguridad" y, por consiguiente, se le excluyera del empleo en cuestión.

La principal aportación que hace el Tribunal es la de incluir la cuestión de la protección de los datos personales dentro del ámbito de la vida privada. Así al señalar que el registro secreto de la policía contenía, sin duda alguna, datos relativos a la vida privada del señor Leander, establecía que "tanto su almacenamiento como su comunicación, unidos a la negativa de permitir al señor Leander que los refutara, suponían una violación del derecho al respeto de su vida privada, garantizado por el art. 8.1" [158].

Con carácter previo, y con una más clara y contundente declaración, la Comisión Europea de Derechos Humanos había establecido en su Parecer sobre este caso, y tomando como base Decisiones previas, que el hecho de que la policía conservara un expediente relativo a un particular y comunicara dicho expediente a un Tribunal constituían una *cuestión de protección de datos que caía dentro del*

[156] *Ibíd.*, p. 482.

[157] El texto de la Sentencia puede verse, en trad. cast., por la que se citará, en BJC. *Tribunal Europeo de Derechos Humanos. Jurisprudencia 1984-1987*, pp. 909-932.

[158] Sentencia Caso Leander, cit., p. 917.

mo en Europa en el curso de los últimos años. Las sociedades democráticas se encuentran amenazadas en nuestros días por formas muy complejas de espionaje y por el terrorismo, de suerte que el Estado debe ser capaz, para combatir eficazmente estas amenazas, de vigilar en secreto las elementos subversivos que operan en su territorio. El Tribunal debe, pues, admitir que la existencia de disposiciones legislativas acordando los poderes de vigilancia secreta de la correspondencia, de los envíos postales y de las telecomunicaciones son, ante una situación excepcional, necesarias en una sociedad democrática para la seguridad nacional y/o la defensa del orden y en la prevención de infracciones penales" [153].

Por otra parte, es necesario verificar si los medios empleados "quedan a este respecto dentro de los límites que son necesarios en una sociedad democrática". Reconociendo al legislador nacional "un cierto poder discrecional" en la elección de las modalidades de vigilancia, el Tribunal estima que le corresponde verificar la existencia de garantías adecuadas y suficientes contra los abusos. Ahora bien, tal poder discrecional no significa que los Estados nacionales dispongan de una discreción ilimitada para controlar con las medidas de vigilancia secreta a las personas sometidas a su jurisdicción. "Consciente del peligro de ver destruir la democracia con el motivo de defenderla, afirma que no sabrían tomar, en nombre de la lucha contra el espionaje y el terrorismo, no importa que medidas juzgadas por ellos apropiadas" [154].

Por ello, la vigilancia secreta debe verificarse en diferentes niveles. Si el carácter secreto de la vigilancia impide al interesado tomar parte directa en el control de tal actividad, se revela imprescindible que los procedimientos existentes proporcionen en sí las garantías apropiadas y equivalentes para la salvaguarda de los derechos del individuo. Se impone consecuentemente el respeto de los valores de una sociedad democrática, entre los que figura la preeminencia del Derecho. Ello implica que una injerencia del ejecutivo en los derechos de los ciudadanos debe verse sometida siempre a un control eficaz [155].

[150] Corte Europea de Derechos Humanos, caso Klass y otros, sentencia de 6 de septiembre de 1978, serie A, núm. 28; recogida, y en trad. cast. de A.J. Martínez Higueras, por la que se citará, en BJC. *Tribunal Europeo de Derechos Humanos 1959-1983*, Secretaría General del Congreso de los Diputados, Madrid, 1984, pp. 470-485.

[151] El art. 8 del CEDH establece:

" 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 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."

[152] Sentencia caso Klass, cit., p. 479.

[153] *Ibíd.*, p. 480.

[154] *Ibíd.*, cit., p. 480.

[155] *Ibíd.*, p. 481.

Para concluir sus alegaciones sobre la cuestión objeto de debate, el Tribunal considera como inherente al sistema del Convenio una cierta forma de conciliación entre los imperativos de defensa de la sociedad democrática y aquellos otros de la salvaguarda de los derechos individuales. Así como declara el Preámbulo del Convenio "el mantenimiento (de las libertades fundamentales) se apoya esencialmente sobre un régimen político verdaderamente democrático, de una parte, y, de otra parte, sobre una concepción común y un común respeto de los derechos del hombre". De acuerdo a lo prescrito en el art. 8 "esto significa que hay que buscar un equilibrio entre el ejercicio por el individuo del derecho (a la intimidad) y la necesidad de imponer una vigilancia secreta para proteger la sociedad democrática en su conjunto"[156].

La línea jurisprudencial abierta por esta sentencia ha sido de una importancia capital. Sus pronunciamientos, aún vigentes en la más moderna jurisprudencia, han posibilitado una visión amplia y realista de los derechos consagrados en el Convenio de 1950.

Así, y con base nuevamente en la posible infracción del art. 8 CEDH, el TEDH se ha pronunciado en el Caso Leander sobre la cuestión de la protección de los datos personales[157].

La sentencia, de 26 de marzo de 1987, tenía como origen la solicitud del señor Leander al no haber podido ocupar un puesto de trabajo debido a la existencia de una serie de antecedentes policiales y políticos en el Registro de la Policía. Estos datos hicieron que se le catalogara como "peligroso para la seguridad" y, por consiguiente, se le excluyera del empleo en cuestión.

La principal aportación que hace el Tribunal es la de incluir la cuestión de la protección de los datos personales dentro del ámbito de la vida privada. Así al señalar que el registro secreto de la policía contenía, sin duda alguna, datos relativos a la vida privada del señor Leander, establecía que "tanto su almacenamiento como su comunicación, unidos a la negativa de permitir al señor Leander que los refutara, suponían una violación del derecho al respeto de su vida privada, garantizado por el art. 8.1" [158].

Con carácter previo, y con una más clara y contundente declaración, la Comisión Europea de Derechos Humanos había establecido en su Parecer sobre este caso, y tomando como base Decisiones previas, que el hecho de que la policía conservara un expediente relativo a un particular y comunicara dicho expediente a un Tribunal constituían una *cuestión de protección de datos que caía dentro del*

[156] *Ibíd.*, p. 482.

[157] El texto de la Sentencia puede verse, en trad. cast., por la que se citará, en BJC. *Tribunal Europeo de Derechos Humanos. Jurisprudencia 1984-1987*, pp. 909-932.

[158] Sentencia Caso Leander, cit., p. 917.

ámbito del artículo 8 [159]. Pero la cuestión no termina ahí y en un examen más exhaustivo, en el que posteriormente no entra el Tribunal, señala como el grado de violación del artículo alegado por el recurrente depende del contenido del registro en cuestión. En el caso que se le somete considera la información registrada en los ficheros policiales como de extrema importancia. Tal extremo se deduce de que la información comunicada afectó gravemente al solicitante al constituir la base de la opinión contraria a su contratación; y sobre todo, por que era referida a actos, asociaciones u opiniones del solicitante y se basaba en una apreciación de su comportamiento o incluso de su personalidad.

Constatada esta violación, tanto la Comisión primero, como el Tribunal después, confluyeron en la misma opinión: la existencia de una justificación a tal injerencia. Tomando como base lo establecido en la Sentencia Klass, se reconoce el objetivo legítimo, la previsión legal y la necesidad de la medida, en una sociedad democrática, para la seguridad nacional.

Pese a que ninguna de las sentencias referidas concluyeron en un planteamiento favorable a los particulares recurrentes, si incorporaron importantes precisiones, que pueden resumirse en:

— se reconoce la inclusión de la protección de datos personales dentro del ámbito de los derechos reconocidos por el art. 8;
— el registro, el almacenamiento y la comunicación de datos personales suponen una violación del derecho al respeto de la vida privada;
— No obstante lo anterior, se posibilita tales medidas cuando se hallen sometidos a determinadas garantías: a) que su realización tenga un finalidad legítima; b) que se hallen previstas legalmente; y c) que su adopción constituya una medida necesaria en una sociedad democrática.

4.1.3. La jurisdicción constitucional española. El corto tránsito hacia la contradicción.

Nuestra jurisdicción constitucional patria no ha sido ajena a los pronunciamientos sobre el derecho a la intimidad, y los posibles ataques a que podía verse sometida por el empleo de las nuevas tecnologías. Aunque con notable retraso respecto a otras jurisdicciones constitucionales de los países de nuestro entorno, también se ha pronunciado sobre la cuestión de la protección de los datos personales, y cúal es su contenido y articulación en el Derecho patrio.

Un lugar destacado en esta labor corresponde a la Sentencia del Tribunal Constitucional 254/1993, de 20 de julio, donde se reconoce y ampara el derecho de los ciudadanos a conocer los datos personales que les conciernen y se hallan registrados en archivos informatizados administrativos. Sus principales aportaciones, junto a la reafirmación de su doctrina tendente al reconocimiento de la aplicación inmediata de los derechos fundamentales, sin necesidad de una *interpositio legislatoris*, pueden sintetizarse, siguiendo la propia línea argumentativa de la Sentencia , en los siguientes puntos:

a. Los riesgos derivados del uso incontrolado de datos personales no pueden ser afrontados eficazmente por los ciudadanos debido a la imposibilidad de conocer que datos sobre sus personas almacenan las distintas Administraciones públicas. Esta situación conlleva también la imposibilidad de conocer y prevenir o perseguir el uso desviado o la diseminación indebida de tales datos, aunque causen lesiones en los derechos e intereses legítimos de los ciudadanos (FJ 4).
b. Para paliar esta situación 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. Instituto que es, 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 provenientes de un uso ilegítimo del tratamiento mecanizado de datos* (FJ 6). El Constitucional señala como la "libertad informática" es el derecho a controlar el uso de los datos insertos en un programa informático (FJ 7).
c. Reconocida la libertad informática, debe procederse al señalamiento de cúal es el contenido mínimo de ese derecho o libertad que el ciudadano debe garantizarse. La protección de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de los ficheros automatizados de la Administración, así como cuales son esos datos personales en poder de las autoridades.

Respecto a la información, ésta ha de ser necesaria para el ejercicio de las potestades que les atribuye la ley, y ser adecuada para las legítimas finalidades previstas (FJ 7).

La importancia de este pronunciamiento jurisprudencial es evidente, por cuanto supuso el reconocimiento jurisdiccional del derecho a la autodeterminación informativa y de los principales rasgos y facultades que lo adornan. Además, conviene tener en cuenta que el fallo, pronunciado tras la entrada en vigor de la LORTAD, supuso también un primer enjuiciamiento, aunque de manera indirecta, de la misma. Puede conceptuarse así como la primera "demanda de acceso". [160]

[159] Parecer de la Comisión Europea de Derechos Humanos, formulado en el informe de la Comisión de 17 de mayo de 1987, y recogido como anexo de la Sentencia Caso Leander, cit., p. 924.

[160] Las consideraciones del TC acerca de los efectos que la aprobación de la LORTAD tiene en el resultado del fallo, se hallan en el FJ 9 de la Sentencia. Un estudio de la referida sentencia, con señalamiento de sus planos argumentativos, puede verse en PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho y Constitución*, cit., p. 368 (nota 24). Asimismo, GONZALEZ 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 los datos personales", en *Informática y Derecho*, núms. 6-7, 1994, pp. 203-248.

Estas aportaciones, no obstante su importancia, quedaron desvirtuadas por el propio Tribunal Constitucional sólo unos meses más tarde con motivo de la Sentencia 143/1994, de 9 de mayo [161]. Planteándose la posible inconstitucionalidad del Número de Identificación Fiscal (NIF), el Tribunal considera que no puede admitirse un derecho absoluto e incondicionado a la reserva de los datos económicos de los contribuyentes con relevancia fiscal, ya que de otro modo se haría imposible la consecución de los fines establecidos por el sistema tributario en el art. 31.1 de nuestra Constitución. Al ser correcta la finalidad perseguida no cabe declarar inconstitucional la norma reguladora del NIF. Ahora bien, como ha hecho notar Pérez Luño, el Tribunal omite pronunciarse acerca del problema que plantean los denominados "identificadores únicos". Los riesgos inherentes a tales "identificadores" derivan fundamentalmente de que su existencia permite una más rápida y eficaz interconexión de ficheros, y ello puede arrojar como precipitado un "perfil de personalidad", prohibido por la mayor parte de las legislaciones del Derecho comparado de la protección de datos. Esta decisión, supone siguiendo nuevamente a Pérez Luño, que desde el punto de vista de la tutela de la libertad informática conformadora del art. 18.4 CE, deba considerarse regresiva respecto a la Sentencia 254/ 1993 [162].

El Tribunal Constitucional se haya, no obstante, en una posición inmejorable para resolver las contradicciones expresadas en las Sentencias referidas anteriormente. El planteamiento de numerosos recursos de inconstitucionalidad contra la LORTAD [163] le va a otorgar una "segunda oportunidad", que esperemos, ahora sí, sirva para delimitar de una manera clara, progresista y eficaz el derecho a la libertad informática en el ordenamiento jurídico español; y, sobre todo, contribuya a hacer realidad en este ámbito lo que proclama nuestro texto constitucional en su art. 9.2, cuando impone a los poderes públicos la promoción de las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas.

4.2. *Leyes de protección de datos y garantías constitucionales.*

Nos saldríamos de los límites asignados a este capítulo si pretendiéramos hacer un análisis extremadamente pormenorizado de las legislaciones nacionales relativas a la protección de los ciudadanos respecto del tratamiento automatizado de los datos personales. Las legislaciones, claramente diversas, surgen en momentos también diferentes, correspondiendo a diversos estados de la técnica informática y, sobre todo, de la conciencia social hacia los peligros que conllevaría un mal uso o abuso de las técnicas automatizadas de tratamiento de datos personales.

Esta evolución y mutación en el contenido y orientación de los productos normativos referentes a la protección de los datos personales ha dado lugar a que se hable, en fórmula paralela a la utilizada con los derechos humanos, de unas *generaciones de leyes de protección de datos.*

Señala Pérez Luño, como con el inicio de la década de los setenta se produce la aparición de una serie de leyes que tienen por objeto la protección de las personas respecto al tratamiento automatizado de los datos de carácter personal [164]. Estas leyes, atendiendo a su orientación y contenido pueden agruparse, en tres generaciones sucesivas:

a. Leyes de la primera generación. Surgieron como instrumentos garantistas encaminados a establecer determinados límites a la utilización de la informática. Su principal objetivo era la reglamentación del funcionamiento de los bancos de datos. Se trataba de leyes generales, que imponían la autorización previa de las bases de datos y el control posterior de su funcionamiento a través de concretos y específicos órganos de vigilancia [165].
b. Leyes de la segunda generación. Su objetivo se centró en asegurar una protección reforzada de determinados datos atendiendo a su calidad. Así incorporaron medidas específicas de protección para los denominados "datos sensibles" por su especial incidencia sobre la vida privada o el ejercicio de las libertades. Su principal aportación radicó, además de lo señalado, en contribuir al reconocimiento y tutela del derecho de acceso y control de los ciudadanos sobre las informaciones personales que les conciernen [166].
c. Leyes de la tercera generación. Se presentan como respuesta a los nuevos problemas tecnológicos y su incidencia en los derechos fundamentales. Los cambios producidos por el desarrollo tecnológico y la importancia alcanzada por el sector informático han condicionado el desarrollo legislativo, tendiendo a buscar un equilibrio entre la protección de los datos personales y la libre circulación de informaciones entre los pueblos. De

[161] Esta Sentencia encuentra un precedente, respecto a los datos relativos a la situación económica de los contribuyentes, en la Sentencia del Tribunal Constitucional 110/1984, de 26 de noviembre. Un interesante estudio de esta Sentencia puede verse en: SANTAMARIA PASTOR, J.A., "Sobre el derecho a la intimidad, secretos y otras cuestiones innombrables", en *Revista Española de Derecho Constitucional,* núm. 15, septiembre-diciembre 1985, pp. 159-180.

[162] *Ibid.*, p. 382 (nota 41).

[163] El Defensor del Pueblo interpuso recurso de inconstitucionalidad el 28 de enero de 1993 (recurso 219/1993). Asimismo han presentado recurso de inconstitucionalidad, el Partido Popular (recurso 236/1993), el Parlamento de Cataluña (recurso 226/1993) y el Consejo Ejecutivo de la Generalidad de Cataluña (recurso 201/1993).

[164] Cfr. PEREZ LUÑO, A.E., "Nuevos derechos fundamentales de la era tecnológica", cit., pp. 178-187.

[165] Cfr. PEREZ LUÑO, A.E., *Libertad informática y leyes de protección de datos*, cit., pp. 145-146 y 152. Se incluirían entre las leyes integrantes de esta primera generación, además de la pionera Ley de Datos del Land de Hesse, la *Data Lag* sueca de 1973 y la *Datenschutz* federal alemana de 1977.

[166] *Ibid.*, pp. 147-149 y 152. Son exponentes de esta segunda generación la *Privacy Act* norteamericana de 1974 y la ley francesa de 1978 relativa a la *Informatique, aux pouvoirs et aux libertés.*

ahí, que al ampliarse las posibilidades de tratamiento automatizado a nivel planetario, gracias a las modernas tecnologías de las telecomunicaciones, sea necesario propiciar un reconocimiento, a escala internacional, de las facultades jurídicas que se derivan del derecho a la libertad informática [167].

En la misma línea por llevar al derecho positivo la garantía de las facultades dimanantes del derecho a la libertad informática se encuadran las primeras, y hasta ahora únicas, consagraciones de este derecho fundamental en las constituciones de Portugal de 1976 y de España de 1978.

La Constitución portuguesa en su art. 35 establece detalladamente normas precisas sobre: a) el derecho de los ciudadanos al conocimiento de los datos que les afectan recogidos en ficheros automatizados y del uso que de los mismos e haga; b) el derecho a la rectificación y actualización de los datos; c) la prohibición del acceso a tales ficheros de terceros; d) la prohibición de la utilización de la informática para el tratamiento de "datos sensibles"; f) la prohibición general de atribución a cada ciudadano de un número nacional de identificación único [168].

En idéntico sentido se manifiesta nuestra vigente Constitución cuando proclama en su art. 18.4 que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Este sucinto planteamiento se halla completado con el reconocimiento del "acceso de los ciudadanos 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 persona", tal y como declara el art. 105 b) [169]. Estas previsiones constitucionales han sido objeto de un posterior desarrollo legislativo en Portugal y España, mediante la promulgación de la Ley 10/91, de 29 de abril de 1991, de protección de datos personales frente a la informática (LPDP); y la Ley Orgánica 5/ 1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), respectivamente.

[167] *Ibíd.*, pp. 149-151 y 152. La *Data Protection Act* inglesa constituye el máximo exponente de esta generación.

[168] Cfr. TONIATTI, R., "Libertad informática y derecho a la protección de los datos personales.", cit., pp. 144-145.

[169] Para un estudio sobre el significado y alcance de estos preceptos constitucionales vid., entre otros: BERMEJO VERA, J., "Premisas de la intimidad personal y de la protección de los datos en el Derecho español" en *Libro Homenaje al Profesor José Luis Villar Palasí,* Civitas, Madrid, 1989, pp. 143-161; CASTELLS ARTECHE, J.M., "La limitación informática", en la obra colectiva *Estudios sobre la Constitución Española.* Homenaje al Prof. Eduardo García de Enterría, Civitas, Madrid, 1991, pp. 907-941; FROSINI, V., "Bancos de datos y tutela de la persona", cit., p. 25.; LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., pp. 150-157; PEREZ LUÑO, A.E., "Informática jurídica y derecho de la informática en España", en *Informática e Diritto,* núm. 2, 1983, pp. 81-99; ID, *Derechos Humanos, Estado de Derecho y Constitución*, cit., pp. 358-383.

4.3. *La proteccion de los datos personales en el ambito internacional.*

Ante la creciente amenaza derivada de los progresos técnicos, las personas afectadas podrían invocar la protección de determinados textos internacionales y especialmente de lo establecido en el art. 12 de la Declaración Universal de Derechos Humanos, el art. 17 del Pacto Internacional relativo a los Derechos Civiles y Políticos y el art. 8 de de la Convención Europea de Derechos Humanos.

No obstante, las mutaciones inevitables introducidas en la vida social y económica por el desarrollo de la informática han determinado que los textos generales que protegen los derechos humanos devengan insuficientes para garantizar los derechos y las libertades fundamentales contra los peligros de las nuevas tecnologías [170].

Estas inquietudes se han resuelto, en un gran número de Estados, como acabamos de exponer, mediante la elaboración de unas legislaciones tendentes a proteger los derechos de los ciudadanos frente a los peligros de la utilización abusiva de la informática.

Ahora bien, la rapidez y la importancia de estos progresos legislativos se vieron pronto en evidencia por efecto del desarrollo del flujo transfronterizo de datos y la globalización del proceso de las comunicaciones [171]. Ante esta nueva situación se planteó la necesidad de elaborar una serie de medidas internacionales de naturaleza homogénea, y que de una u otra manera vinculara a los Estados en el desarrollo de sus políticas. Sólo así podría conseguirse una protección adecuada de los intereses ciudadanos, al margen de los particularismos localistas.

Además, como tuvimos ocasión de apuntar anteriormente, las modernas tecnologías de la comunicación han posibilitado una transmisión de datos a nivel planetario, lo cual exige un reconocimiento global de las facultades que dimanan del derecho a la libertad informática.

Sucesivamente, la Organización para la Cooperación y el Desarrollo Económico (OCDE), el Consejo de Europa y la Comunidad Europea, cada uno en su ámbito y a su manera, han intervenido para trata de paliar los problemas anteriormente apuntados.

No entrando ahora en la regulación comunitaria de la protección de los datos personales, que será objeto de un estudio específico y detallado más adelante, abordaremos a continuación el estudio de las principales aportaciones surgidas del resto de sistemas normativos internacionales precitados.

[170] Cfr. FOCSANEANU, L., "La protection des données à caractère personnel contre l´utilisation abusive de l´informatique", en *Journal du Droit International,* núm. 1, 1982, p. 56.

[171] Cfr. BUQUICCHIO, G., "Informática y libertades. Balance de quince años de actividad del Consejo de Europa", trad. cast. de I. Hernando, en Actas de las *Jornadas Internacionales sobre Informática y Administración Pública,* Instituto Vasco de Administración Pública, Oñati, 1986, p. 99.

4.3.1. La Recomendación del Consejo de la OCDE de 1980. [172]

Las líneas directivas señaladas por la Recomendación no presentan un carácter obligatorio desde el punto de vista jurídico, tal y como declara la Exposición de motivos. Su contenido es el resultado de un consenso sobre unos principios fundamentales que podían ser integrados en las legislaciones nacionales o servir de base a las legislaciones de los Estados que carecían de una ley nacional de protección de datos.

Sus líneas directrices se sintetizan en:

a) El ámbito subjetivo de aplicación se limita únicamente a las personas físicas.
b) El ámbito material de aplicación afecta tanto a los ficheros del sector público, como a los del sector privado.
c) Los Estados miembros están facultados para: 1) aplicar a diferentes categorías de datos medidas de protección diferentes; 2) excluir de las garantías a determinados datos que no presenten manifiestamente ningún riesgo para las libertades individuales; 3) limitar la aplicación de las medidas adoptadas a los ficheros automatizados, con exclusión de los manuales.
d) Las líneas establecidas en la Recomendación constituyen normas mínimas susceptibles de ser completadas por otras medidas más amplias.

La Recomendación establece también una serie de principios fundamentales aplicables tanto en el plano nacional, como en el internacional. Respecto a los primeros destacan: 1. Principio de limitación en la recogida de datos; 2. Principio de cualidad de los datos; 3. Principio de especificación de las finalidades; 4. Principio de limitación del uso de los datos; 5. Principio de garantía de la seguridad; 6. Principio de transparencia ; 7. Principio de reconocimiento a toda persona física de los derechos de información, acceso, rectificación y cancelación; 8. Principio de responsabilidad del responsable del fichero.

Los principios relativos a la libre circulación de los datos personales en el plano internacional se refieran a: 1. Necesaria toma en consideración de los intereses de otros Estados miembros; 2. Libre circulación y libre flujo de datos personales; 3. Posibilidades de restricción al flujo transfronterizo de datos; 4. Prohibición del abuso de derecho.

La Recomendación se cierra con unas indicaciones sobre la puesta en vigor de las líneas señaladas anteriormente, así como de las medidas para establecer un marco de cooperación internacional en materia de protección de datos.

[172] *Flujo internacional de Datos. Recomendación de la OCDE de 23 de septiembre de 1980*, Documentación Informática, nº 2, Servicio Central de Publicaciones - Presidencia del Gobierno, Madrid, 1983.

4.3.2. 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. [173]

El Convenio establece en su Preámbulo la necesidad de proteger "el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamiento automatizado". Ahora bien, debe hacerse "reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos".

Partiendo de estos postulados, el Convenio en su art. 1 señala cúal sea su *objeto y fin*, que se concreta en "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o 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 personas". Su *ámbito de aplicación* se extiende a los sectores públicos y privados (art. 3).

Entre los *Principios básicos para la protección de los datos*, se establecen criterios relativos a la calidad de los datos, entendiendo que han de ser exactos, actualizados (si fuera necesario), adecuados y proporcionados a su finalidad legítima y determinada y obtenidos y tratados legal y legítimamente (art. 5). Asimismo, aportación muy importante del Convenio, se prohíbe el tratamiento, a menos que los Derechos nacionales prevean garantías suficientes, de los llamados *datos sensibles*; es decir, de aquéllos que revelen el origen racial, las opiniones políticas, las convicciones religiosas o de otro tipo, así como los datos relativos a la salud o a la vida sexual. Esta prohibición se extiende igualmente a los datos personales referentes a condenas penales (art. 6).

Asumiendo una línea garantista, el art. 7 fija criterios sobre la *seguridad de los datos*, en tanto que el art. 8 establece unas *garantías complementarias para la persona concernida*, que se concretan en los derechos de información, acceso, rectificación y borrado.

Se recoge la posibilidad de *restricciones y excepciones*, cuando los derechos derivados de los principios básicos indicados entren en conflicto con otros intereses (seguridad del Estado, seguridad pública, intereses monetarios del Estado, represión de infracciones penales, protección de la propia persona concernida y derechos y libertades de terceros, todo ello siempre "que constituya una medida necesaria en una sociedad democrática") (art.9). Como contrapartida se establece la posibilidad de los Estados miembros para establecer medidas de protección de mayor amplitud y eficacia (art. 11).

[173] *Protección de datos. Convenio del Consejo de Europa de 1981*, Documentación Informática, nº 3, Servicio Central de Publicaciones - Presidencia del Gobierno, Madrid, 1983.

Su art. 10 señala la obligación para las Partes Contratantes de establecer las oportunas *sanciones y recursos* para los supuestos de violación de las disposiciones que en el Derecho interno desarrollen los principios establecidos por el Convenio.

Otras disposiciones sobre *flujos internacionales de datos* (art. 14), *cooperación entre las Partes* (art. 13), *asistencia a personas concernidas residentes en el extranjero* (arts. 14-17), así como la formación de un *Comité Consultivo* a quien se encomienda la formulación de propuestas encaminadas a modificar el Convenio, a mejorar su aplicación y la elaboración de informes sobre la materia (arts. 18-20), completan la exposición de un texto internacional de indudable relevancia, cuyos contenidos han servido, no sólo de modelo y guía, sino también de auténtico acicate, para la elaboración de numerosas leyes nacionales de protección de datos [174].

Al margen de este Convenio el Consejo de Europa ha elaborado una serie de Recomendaciones que, tomando como punto de partida lo establecido en el texto del Convenio de 1981, pretenden adaptar la protección de los datos personales a las necesidades propias de determinados tratamientos automatizados de datos [175].

[174] Sobre el contenido, relevancia y eficacia del Convenio, vid., entre otros: FOCSANEANU, L. "La protection des données à caractère personnel...", cit., pp. 75-95; GARZON CLARIANA, G., "La protección de los datos personales y la función normativa del Consejo de Europa", en *Revista de Instituciones Europeas*, vol. 8, núm. 1, enero-abril 1991, pp. 9-ss; HEREDERO HIGUERAS, M., "Ante la ratificación del Convenio de protección de datos del Consejo de Europa", en *Documentación Administrativa*, núm. 199, 1983, pp. 753-ss.; LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa,* cit., pp. 140-144; RIGAUX, F; "La loi applicable à la protection des individus à l´égard du traitement automatisé des données à caractère personnel", en *Revue Critique de Droit International Privé*, núm. 3, 1980, pp. 430-ss; PEREZ LUÑO, A.E., "La incorporación del Convenio europeo sobre protección de datos al ordenamiento jurídico español", en *ICADE. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales,* núm. 17, 1989. pp. 27-ss; RIPOLL CARULLA, S., "El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal: Balance a los siete años de su apertura a la firma", en Actas del *Congreso sobre Derecho Informático*, Facultad de Derecho, Zaragoza, 1989, pp. 395-413; *ID, Las libertades de información y de comunicación en Europa*, Tecnos & Fundación Cultural Enrique Luño Peña, Madrid, 1995.

[175] Recomendación (83) 10, de 23 de septiembre de 1983, sobre la protección de datos personales frente a su uso con fines científicos o estadísticos; Recomendación (85) 20, de 25 de octubre de 1985, sobre la protección de datos personales frente a su uso para marketing directo; Recomendación (87) 1, de 23 de enero de 1986, sobre protección de datos personales frente a su uso para fines de seguridad social; Recomendación (87) 15, de 17 de septiembre de 1987, sobre utilización de datos personales por la policía; Recomendación (89) 2, de 18 de enero de 1989, sobre protección de datos personales utilizados con fines de empleo; Recomendación (91) 19, de 13 de septiembre de 1990, sobre la protección de los datos de carácter personal utilizados con fines de pago y otras operaciones conexas; Recomendación (91) 10, de 9 de septiembre de 1991, sobre la comunicación a terceros de datos de carácter personal en poder de organismos públicos; y Recomendación (95) 4, de 7 de febrero de 1995, sobre la protección de los datos de carácter personal en el ámbito de los servicios de telecomunicación, en especial con relación a los servicios telefónicos. Recomendación (95) 11, de 11 de septiembre, relativa a la selección, tratamiento, presentación y archivo de las

5. EL CONTENIDO DEL DERECHO A LA LIBERTAD INFORMÁTICA: PRINCIPIOS, DERECHOS Y GARANTIAS.

El contenido típico del derecho a la libertad informática está integrado, como señala Lucas Murillo de la Cueva, por las diferentes facultades y poderes de control que se reconocen a sus titulares sobre las informaciones personales que les atañen, así como los deberes y obligaciones que pesan sobre los sujetos pasivos, y por las garantías objetivas, procedimientos e instituciones de garantía previstas por el legislador [176].

Facultades y poderes que abarcan todas las fases de elaboración y uso de datos; es decir, su acumulación, su transmisión, su modificación y su cancelación [177].

Esta concepción global - en todo el ciclo operativo del tratamiento automatizado de datos - no es más que la emanación de la necesaria concepción global de los problemas inherentes a la protección de los datos personales; y en ese sentido deben entenderse las reflexiones que a continuación desarrollamos.

5.1. *Principios de la proteccion de datos.*

El Convenio del Consejo de Europa de 1981 sobre protección de datos (en adelante, el Convenio), al que nos hemos referido en el capítulo precedente, incluye entre sus aspectos relevantes el haber incorporado un elenco de los principios a los que debe atemperarse el tratamiento automatizado de datos personales para salvaguardar los derechos y libertades de los ciudadanos [178].

Estos principios, recogidos en todas las legislaciones nacionales sobre protección de datos, son interdependientes y en parte se entrecruzan y traspasan. Es por ello que las distinciones que con relación a los principios se hacen sean consideradas como artificiales, y no deben ser obstáculo para la consideración conjunta de los principios y que su tratamiento sea estudiado como un todo.

resoluciones judiciales en los sistemas de documentación jurídica automatizada. Recomendación (97) 5, de 13 de febrero, relativa a protección de datos médicos.

El texto integro de estas Recomendaciones puede verse en HEREDERO HIGUERAS, M., *La Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal. Comentario y Textos*, Tecnos, Madrid, 1996. Asimismo en El Consejo de Europa y la protección de datos personales, Agencia de Protección de Datos, Madrid, 1997.

[176] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, cit., p. 55.

[177] Cfr. DENNINGER, E., "El derecho a la autodeterminación informativa", cit., p. 273; PEREZ LUÑO, A.E., "Informática jurídica y Derecho de la informática en España", cit., p. 94.

[178] Cfr. ESTADELLA, O., *La protección de la intimidad frente a la transmisión internacional de datos personales*, Tecnos & Generalitat de Catalunya. Centro d´Investigació de la Comunicació; Madrid, 1995, especialmente pp. 82-104; RIPOLL CARULLA, S., *Las libertades de información y de comunicación en Europa*, Tecnos & Fundación Cultural Enrique Luño Peña, Madrid, 1995.

Dos reglas fundamentales pueden extraerse de la asunción de estos principios. Por un lado, la información debe ser correcta, pertiente y no excesiva, con relación a su fin; por otra, su utilización debe ser igualmente correcta.

En idéntica concordancia con lo establecido por el art. 5 del Convenio [179], pueden señalarse los siguientes principios, que deben inspirar no sólo la acción legislativa, sino que se imponen como de inexcusable cumplimiento para todos aquellos que intervengan en un tratamiento automatizado de datos personales.

5.1.1. Principio de recogida y tratamiento leal y lícito.

La lealtad y la licitud son las cualidades esenciales de la operación consistente en almacenar datos personales para someterlos a un tratamiento automatizado.

La lealtad se refiere, especialmente, a las circunstancias en las que los datos han sido obtenidos, a la legitimidad de las finalidades perseguidas por el tratamiento y a la pertinecia de los datos recogidos, medida en relación con sus finalidades [180].

Las nuevas tecnologías ofrecen nuevos medios de recogida de datos: al suministro de datos procedentes de declaraciones de todo tipo, formularios, solicitudes, se unen actualmente los generados por la utilización de determinadas redes y sistemas informáticos.

Respecto a la información recogida, debe establecerse para los solicitantes o destinatarios de los datos, la obligación de informar a la persona "interrogada" del carácter obligatorio, o facultativo de sus respuestas, de las consecuencias derivadas de su falta de respuesta, de las personas físicas o jurídicas destinatarias de los datos, de la existencia de un derecho de acceso y rectificación.

Esta información permitirá a la persona cuyas informaciones sean solicitadas ejercer, de forma inmediata, el derecho de oponerse por razones legítimas al tratamiento de estas informaciones o a su registro en un banco de datos. Le permite subsidiariamente, si no puede ejercitar ese derecho de oposición, ejercer los derechos de acceso, comunicación y rectificación sobre las informaciones recogidas que le atañen [181].

Ahora bien, lo que se denomina un procedimiento de recogida lícita y leal dependerá sobre todo de los procedimientos técnicos utilizados para la recogida y registro de los datos. Y esta problemática se manifiesta de manera especial cuando nos estamos refiriendo a datos obtenidos mediante mecanismos ocultos, tales como videograbadoras, magnetófonos o cualesquiera otros que induzcan a error a los interesados respecto al destino final de su uso. En estos supuesto, dos ideas deben ser tenidas en cuenta: 1. la transparencia; 2. el consentimiento. La necesidad de poner los datos en conocimiento del interesado o de obtener su consentimiento para registrarlos, constituye una norma básica que se concreta en la necesidad de un "consentimiento libre e informado" de la persona concernida.

No debe olvidarse, por último, que las nuevas tecnologías, cuya manifestación más relevante son las autopistas de la información, requerirán de una novedosa solución a nivel legislativo antes que esos datos puedan ser recogidos [182]. Y debe ser con carácter preventivo como se salvaguardan la lealtad y licitud del tratamiento de datos. Con posterioridad, dichos datos se integrarán en el macrosistema, se diluirán entre los múltiples entradas y salidas y será *de facto* imposible seguirles la pista.

5.1.2. Principio de determinación de la finalidad.

Este principio implica, ante todo, que antes de su puesta en funcionamiento la finalidad de los ficheros debe ser indicada, a fin de que pueda verificarse si los datos registrados están en conexión con esta finalidad; si no están siendo utilizados con otros fines que aquellos para los que inicialmente fueren recabados; y si la duración del plazo de conservación no excede de aquélla que permite salvaguardar la finalidad enunciada [183].

La determinación de las finalidades puede revestir diversas modalidades, y variar según el derecho interno. No obstante, si conviene tener en cuenta que los

[179] Artículo 5 (Calidad de los datos).
"Los datos de carácter personal que fueren objeto de un tratamiento automatizado deberán ser:
a) Obtenidos y elaborados leal y lícitamente.
b) Registrados para unos fines determinados y legítimos y no utilizados de manera incompatible con tales fines.
c) Adecuados, pertinentes y no excesivos con respecto a los fines para los que fueron registrados.
d) Exactos y, si fuere necesario, tenidos al día.
e) Conservados en forma que permitiere la identificación de los interesados durante un plazo que no excediere del necesario para los fines para los cuales fueren registrados."

[180] Cfr. RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, cit., p. 585.

[181] Cfr. KAYSER, P., *La protection de la vie privée*, 2º edit., Económica, Paris, 1990, pp. 351-352.

[182] Vid. sobre extremo, en el ámbito comunitario europeo: Propuesta modificada de Directiva del Parlamento Europeo y del Consejo relativa a la protección de los datos personales y la intimidad en relación con las redes digitales de telecomunicación y, en particular, la Red digital de Servicios Integrados (RDSI) y las redes móviles digitales públicas, COM(94) 128 final/2-COD 288, Bruselas, 15.06.1994; COLOM, V. y VAN BOLHIUS, H.E., *Cyberspace Reflections*, European Commission. DG XIII, Bruselas, 1995.

[183] Cfr. MAISL, H., "État de la législation française et tendances de la jurisprudence relatives a la protection des données personnelles", en *Revue Internationale de Droit Comparé*, núm. 3, juillet-septembre 1987, p. 570.

tratamientos automatizados de datos personales tienen, generalmente y en principio, una única finalidad. Ello implica que los datos que fueran dados para una determinada función o razón no pueden ser utilizados para otras diferentes. Esta determinación únivoca de la finalidad implica, además, como valor añadido:

a. la interdicción previa del registro de datos para fines no determinados;
b. la necesaria especificación, en aquellos casos excepcionales y predeterminados por la ley, de los supuestos de modificación posterior de las finalidades previamente determinadas. Las nuevas finalidades no deberán añadirse, no obstante, de manera arbitraria, sino que debe implicar la compatibilidad de los nuevos fines con los iniciales.

Especial atención debe prestarse a las posibilidades de interconexión y transmisión de datos de/entre ficheros. Tratamientos, en principio, respetuosos con el principio de determinación de la finalidad, pueden ver desvirtuada por esta posibilidad su adecuación con la normativa protectora y constituir una importante brecha en el sistema de garantías.

De esta forma, datos recabados inicialmente con finalidad de facturación de determinados servicios, en numerosas ocasiones de naturaleza pública, incorporan también, por la propia naturaleza del servicio recibido o prestado, indicaciones sobre los gustos y los hábitos de las personas; y son susceptibles, por tanto, de una utilización secundaria. Se genera, ante tal posibilidad, que otros prestadores de servicios podrán tener interés por los referidos datos en función de sus particulares actividades económicas y/o comerciales. Ejemplo paradigmático de este supuesto lo constituye la utilización por parte del sector bancario de los datos sobre la capacidad y solvencia económica de sus clientes, para la oferta de determinados productos de aseguramiento personal, familiar o profesional. No debe olvidarse que los grandes bancos son, a la postre, los propietarios - o al menos un sector importante del accionariado - de las grandes compañias de seguros.

La necesidad de almacenamiento de esos datos por motivos de gestión económica de los prestadores de servicios, no debe esconder una subversión de la finalidad para la que fueron recabados y almacenados los datos. Como ha señalado Pérez Luño, no es aceptable que informaciones recabadas y publicadas en función de intereses colectivos y sociales puedan ser incontrolada e impunemente utilizadas para fines e intereses privados comerciales y, por tanto, ajenos a aquellos que justificaron su recogida y su publicidad [184].

Esta situación requiere un decidido control sobre las bases de datos y los procedimientos y protocolos técnicos de transmisión e interconexión de datos. Como ha señalado Denninger, "la falta de determinar la finalidad concreta de una transmisión de datos o una formulación demasiado general podía llevar a una situación tal que en un principio la evaluación de datos y su acumulación se efectúe con un fin concreto, pero que estos datos después puedan ser consultados y transmitidos para cualquier fin sin que la persona concernida pudiera influir sobre ellos" [185].

Otro aspecto a destacar es que cuando los datos hubieren dejado de estar subordinados a un fin, por consecución, desviación o imposibilidad del mismo, deberá procederse a su destrucción o, y sólo en casos muy taxados, a su conservación en forma anónima. La razón radica en que cuando los datos dejan de ser especialmente relevantes se baja la guardia, y es cuando se producen los mayores riesgos de una utilización ilícita de los mismos [186].

Por último, no conviene olvidar que si el principio de la finalidad definido en el Convenio resulta operativo en el contexto de las nuevas tecnologías, parece necesario el establecimiento de garantías suplementarias en lo referente a las nuevas técnicas interactivas, ante la imposibilidad de proceder a un verdadero control del respeto de la finalidad dado el gran número de datos almacenados y tratados y la multiplicación de servicios ofertados por los medios interactivos.

5.1.3. Principio de calidad de los datos.

Los datos habrán de ser adecuados, pertinentes y no excesivos con respecto a los fines para los que fueron registrados. Asimismo deberán ser exactos y, cuando fuere preciso, actualizados.

Se revela conveniente poner los datos en relación con la finalidad para la cual han de ser utilizados, para determinar, como criterio cualitativo, la pertinencia y adecuación del tratamiento. Así los datos relativos a opiniones o valoraciones personales pueden inducir a error si se utilizan para finalidades distintas de aquellas para las que fueron recabados, y con las que no guardan ningún genero de relación.

Igualmente el "principio de finalidad" será el relevante para la determinación de los datos como excesivos. Este criterio cuantitativo, hace referencia al conjunto de los datos estrictamente necesarios para el cumplimiento de una finalidad previamente determinada. De este modo, el alcance de los datos no deberá exceder en ningún caso del necesario para cumplir la finalidad con motivo de la cual fueren a utilizarse los referidos datos.

Respecto al principio de exactitud, considerado como criterio material respecto de la información que incorporan los datos, es importante asegurar que los datos objeto de un tratamiento no aparezcan deformados. El problema de la exactitud se plantea igualmente en el momento de la recogida como en el de transmi-

[184] Cfr. PEREZ LUÑO, A.E., "Comentario Legislativo: La LORTAD y los derechos fundamentales", en *Derechos y Libertades*, núm. 1, febrero-octubre 1993, p. 418.

[185] Cfr. DENNINGER, E., "El derecho a la autodeterminación informativa", cit., p. 273.
[186] Cfr. *Flujo internacional de datos: Recomendación de la OCDE...*, cit., p. 53.

sión de los datos. La transmisión, por ejemplo de datos policiales o médicos inexactos, puede tener graves consecuencias. En todos los casos, parece importante que los ciudadanos dispongan de un derecho de información y acceso sobre los datos que les conciernen, para verificar si tal calidad se cumple.

El principio de exactitud deviene especialmente relevante para enjuiciar los denominados "perfiles de la personalidad", establecidos a partir de informaciones recogidas sobre una persona. La interconexión de datos, recogidos hasta entonces de manera dispersa, arrojan como precipitado una imagen de nuestra propia personalidad, que en numerosas ocasiones no se corresponde ciertamente con nuestros hábitos y actitudes vitales. Tales datos no son más que un aspecto puntual y concreto, cuando no contigente, de determinadas manifestaciones de nuestra vida personal y social. No debe olvidarse, como señala Rigaux, que las diversas actitudes que, por su convergencia, forman un perfil, son, tomados cada uno aisladamente, manifestación del ejercicio de una libertad de autodeterminación que, protegidos por las leyes, pertenecen a todos los individuos [187].

En todo caso, el establecimiento de tales perfiles no debería permitir la elaboración de un juicio sobre una persona. La transmisión de tales informaciones debe igualmente acompañarse de garantías adecuadas, tales como la impugnación de las valoraciones que les resulten perjudiciales y que se basen exclusivamente en un tratamiento automatizado que de un perfil de su personalidad.

Por tanto, en la medida en que el principio de exactitud sea respetado, y donde la transmisión de datos sea cuidadosamente regulada, el establecimiento de perfiles sobre los individuos perderá gran parte de de su fuerza como elemento lesivo para los derechos de los individuos.

(4) Por otro lado, el respeto de estos principios implica para los responsables del fichero la obligación de cancelación, *ex officio* o a instancia del interesado, de los datos inexactos o incompletos y, en su caso, su sustitución por los datos rectificados o completados [188]. Los responsables de los ficheros deberán observar, de esta forma, un especial deber de diligencia y efectuar las correcciones necesarias para adecuar el tratamiento a los principios establecidos por las normas tutelares de los datos personales.

5.1.4. Principio de conservación limitada de los datos.

Este principio se aplica fundamentalmente a aquellos datos nominativos que permitan la identificación del interresado. El establecimiento de un tiempo máximo de conservación de datos personales tiene por objeto asegurar a los individuos

[187] Cfr. RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, cit., p. 431.
[188] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, cit., p. 67.

que determinados actos, manifestaciones u opiniones, no van a suponer un elemento universal y eterno, que condicione de manera permanente y coarte sus posibilidades de evolución personal y social.

Es lo que habitualmente se conoce como *"derecho al olvido"* [189]. No obstante el derecho al olvido no debe significar destrucción de datos que constituyan elementos de la conciencia histórica y social [190]. Estos datos podrían devenir anónimos y ser utilizados por los investigadores en los diferentes campos del saber.

Ahora bien, el problema fundamental radica en saber *a priori* que datos van a alcanzar, transcurrido un determinado tiempo, el rango de relevantes para la historia y conciencia social; y cuales de aquellos, que en el momento de su conservación parecian asegurar tal interés, quedarán, por el mismo transcurso del tiempo, reducidos a meras indicaciones de modas pasajeras o tendencias irrelevantes para el decurso, histórico, social y/o cultural.

El "derecho al olvido" consistirá, de acuerdo a lo expresado, en hacer inaccesible los datos registrados en un fichero transcurrido el tiempo predeterminado por la ley o el acordado entre las partes. Ahora bien, como ha señalado el Convenio 108 del Consejo de Europa, ello no significa que, transcurrido algún tiempo, deban separarse irrevocablemente del nombre de la persona a la cual hicieren referencia, sino que no deberá ser posible relacionar los datos y los identificadores [191].

El periodo de conservación debe estar previsto desde el comienzo del tratamiento; y debe conectarse con la finalidad para la cual los datos han sido registrados.

Desde el punto de vista de los individuos afectados, transcurrido el plazo predeterminado, recupera la plena disposición sobre la información que le concierne; debiendo producirse por parte del responsable del fichero la cancelación de los registros que la contuvieran [192].

El aseguramiento del cumplimiento de conservación limitada de los datos personales debe constituir una preocupación constante, por cuanto la difusión de informaciones descontextualizadas y obsoletas pueden acarrear perjuicios considerables a los ciudadanos.

[189] Cfr. KAYSER, P., *La protecion de la vie privée*, cit., p. 355.
[190] Cfr. MAISL, H., "Etat de la legislation française et tendances de la jurisprudence relatives a la protection des données personnelles", en *Revue Internationale de Droit Comparé*, nº 3, juillet-septembre 1987, p. 574.
[191] Cfr. *Protección de datos. Convenio del Consejo de Europa de 1981*, cit., p. 32.
[192] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, cit., p. 68.

5.1.5. Principio de restricción de uso.

La determinación del uso que va a realizarse de los datos constituye una garantía para los ciudadanos que se traduce en la necesaria información, en el momento de la recogida, acerca de la finalidad de la misma, así como de las operaciones materiales y lógicas empledas en las diferentes fases del tratamiento automatizado.

Conectado con el "principio de determinación de la finalidad" nos permitirá determinar que usos de los datos constituyen una clara y manifiesta desviación de los necesarios principios a los que deberá atemperarse todo tratamiento de datos.

De este modo el uso de los datos deviene criterio material y previo al de finalidad; al señalar la regla lógica de conexión entre la recogida de datos y la consecución teleológica de un resultado. Se trata, en definitiva, de asegurar por parte de los reponsables de los ficheros, la necesaria coherencia lógica entre presupuestos y resultados en un proceso de tratamiento automatizado de datos personales.

5.2. *Los derechos de la persona afectada.*

Constituyen el núcleo del sistema de garantías en torno a las cuales se articula el derecho a la libertad informática. Junto al escrupuloso respeto de los principios a los que debe someterse un tratamiento automatizado de datos, deben garantizarse una serie de derechos de los ciudadanos en relación con la información que les atañe. Su objetivo general es poner coto a una situación, en muchos casos de absoluta indefensión, en la que los ciudadanos no tenemos ni siquiera conocimiento de la lesión de nuestros derechos, hasta que sufrimos las consecuencias en nuestra vida cotidiana (negación de determinadas solicitudes o prestaciones, inclusión en "censos negros", "bombardeo" publicitario, etc.) debido a un uso torticero, excesivo o incompleto de nuestros datos personales [193].

Se trata, en definitiva, de la articulación de una serie de mecanismos de garantía de los que los titulares del derecho a la libertad informática pueden usar para salvaguardar sus intereses frente a quienes mantienen ficheros automatizados de información personal, o se dedican a su tratamiento, comunicación, transmisión o cesión [194], y cuyo conocimiento y difusión pueden o no interesar a los que tratan los datos o a la sociedad [195].

[193] Cfr. MADRID CONESA, F., *Derecho a la intimidad, informática y Estado de Derecho*, cit., p. 84.
[194] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, cit., p. 74.
[195] Cfr. OROZCO PARDO, G., "Consideraciones sobre los derechos de acceso y rectificación en el proyecto de Ley Orgánica de Regulación del tratamiento automatizado de los datos de carácter personal", en *Actas del III Congreso Iberoamericano de Informática y Derecho* (Mérida, septiembre 1992), publicadas en *Informática y Derecho*, núm. 4, 1994, p. 215.

Pérez Luño ha señalado como una de las principales aportaciones de las legislaciones de protección de datos el reconocimiento y tutela jurídica que éstas hacen del derecho a la libertad informática. Derecho de autotutela sobre las informaciones personales, cuya función se cifra en garantizar a los ciudadanos una facultades de información, acceso y control de los datos que les conciernen [196].

Conceptuados claramente como derechos subjetivos, buscan de una manera muy concreta un equilibrio entre los "fichadores" y los "fichados", otorgando a éstos últimos una serie de derechos de novedosa configuración, y que son susceptibles de ejercitarse, tanto en el momento de la recogida de la información, como en el momento de su tratamiento [197].

Ahora bien, este conjunto de derechos configura un *status* personal, integrador del derecho a la libertad informática y que abarca todas las facultades del individuo sobre las informaciones que le conciernen. En un plano más restringido, con el que no debe confundirse, se manifesta el denominado *status* de *habeas data*, principal instrumento de garantía de la libertad informática y que se manifiesta en la facultad de las personas en conocer y controlar las informaciones que les conciernen procesadas en bancos informatizados [198].

En la actualidad la consagración del derecho a la libertad informática, en el seno de los derechos de la tercera generación, ha determinado que se postule el *status* de *habeas data*, como cauce procesal para salvaguardar la libertad de las personas en la esfera informática. Y es ahí precisamente donde radica su función: garantía de acceso y control sobre las informaciones personales por parte de las personas concernidas. Pero, como hemos señalado, la libertad informática, como categoría más amplia y que acoge en su seno, entre otros al *status* de *habeas data*, implica otras facultades tales, como exigir la rectificación de los datos incorrectos, el borrado de datos "indebidos", etc.., en la forma que a continuación desglosamos.

Establecida esta puntual e imprescindible aclaración, que por nada debe considerarse baladí, estos derechos pueden reconducirse a las siguientes categorías, que a continuación expondremos.

5.2.1. Derecho de Información.

Denominado también como "principio de transparencia", puede ser considerado como condición previa para el ejercicio de los demás derechos reconocidos a

[196] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho y Constitución*, cit., p. 378; ID, "Comentario Legislativo: La LORTAD...", cit., p. 419.
[197] Cfr. MAISL, H.,"Etat de la legislation française et tendances...", cit., p. 576.
[198] Cfr. PEREZ LUÑO, A.E., "Del *Habeas Corpus* al *Habeas Data*", en *Informática y Derecho*, núm. 1, 1992, p. 158 ; ID., "Intimidad y protección de datos personales: Del *Habeas Corpus* al *Habeas Data*", cit., p. 40.

los ciudadanos. Para que éstos puedan ser aplicados eficazmente se requiere que sea posible en la práctica adquirir información sobre la recogida, almacenamiento o uso de los datos personales.

Esta posibilidad genérica se resuelve para los ciudadanos en la posibilidad de conocer la existencia de un fichero, identidad y dirección de su responsable, finalidad de la recogida de datos, destinatarios de la información, carácter obligatorio o facultativo de la respuesta, consecuencias de la obtención de datos o de la negativa a facilitarlos [199]. Igualmente debe informarse de los derechos que le asisten en materia de protección de datos de carácter personal, así como de las formas y modalidades de su ejercicio.

Estas facultades reconocidas a los particulares incorporan como contrapartida la obligación para los bancos de datos de un status de publicidad [200] que se concretará, bien en la inscripción del responsable del fichero en un registro público; o bien, para los Estados que carezcan de tal registro, por el suministro al particular que lo solicitare del nombre y demás menciones referentes al responsable del fichero.

La mayoría de las leyes de protección de datos incorporan entre sus previsiones la creación de un Registro donde deberán inscribirse todos aquellos ficheros que traten datos personales, con descripción de las actividades relativas al tratamiento, tanto subjetivas como materiales. Generalmente, estas menciones vienen predeterminadas por las propias leyes, que establecerán así un modelo unitario del contenido de la referida inscripción.

Tal criterio unitario, y por ende el propio Registro, cumplen de esta forma una doble e importante misión: 1) asegurar la uniformidad de las modalidades de ejercicio del derecho de información, obviando los problemas de seguridad jurídica que pudieran plantearse si cada operador informático suministrara los datos que, según su propio y generalmente restrictivo criterio, considerara relevantes; 2) asegurar que el derecho de información pueda ejercitarse de manera real y efectiva, sabiendo a quien tenemos que dirigirnos y qué información podemos reclamarles.

Las menciones incluidas en el registro son generalmente publicadas para general conocimiento, constituyéndose como un instrumento necesario para hacer efectivo el derecho de información.

Pero si afirmamos que no basta cualquier mención en el Registro para colmar las exigencias de información, tampoco basta, por mera coherencia interna, cualquier mención en la publicación de los datos obrantes en el registro. Es a través de

[199] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., p. 187; *ID, Informática y protección de datos personales*, cit., p. 62.

[200] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., p. 187.

esta publicidad como los ciudadanos toman conocimiento de la existencia de los ficheros y de los derechos que le asisten con respecto a ellos.

Así, en la mayoría de los países con legislaciones protectoras de datos personales automatizados las inscripciones registrales son publicadas para general conocimiento. Tal es el supuesto que recientemente ha tenido lugar en nuestro país, tras la publicación de la primera edición de la relación de ficheros automatizados de datos de carácter personal [201].

El art. 26.2 e) del Estatuto de la Agencia de Protección de Datos [202] señala de entre las funciones del Registro de Protección de Datos la de publicar una relación de los ficheros notificados e inscritos. Respecto a la inscripción, el art. 24.2 del referido Estatuto señala como en los asientos de inscripción de los ficheros de titularidad pública deberán constar las informaciones a que se refiere el art. 18.2 de la LORTAD [203]; en los de titularidad privada, los extremos exigidos por el art. 24.2 de la referida Ley Orgánica [204]. En todo caso, deberán figurar aquellos datos que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación (art. 24.4 del Estatuto de la Agencia).

Este coherente régimen se vió sin embargo menoscabado gravemente cuando, al dirigirnos a los gruesos volúmenes en que se recogían el listado de ficheros comunicados al Registro, no encontrabamos casi ninguna de las menciones requeridas por la propia LORTAD. Sólo aparecían el nombre del titular del fiche-

[201] Cfr. Registro General de Protección de Datos, *Ficheros automatizados de datos de carácter personal. Titularidad Pública (1994-95)*, Vol. I, Agencia Española de Protección de Datos & Boletín Oficial del Estado, Madrid 1995; *ID, Ficheros automatizados de datos de carácter personal. Titularidad Privada (1994-95)*, Vol. II, Agencia Española de Protección de Datos & Boletín Oficial del Estado, Madrid, 1995.

[202] Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, publicado en el BOE núm. 106, de 4 de mayo de 1993.

[203] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, publicada en el BOE núm. 262, de 31 de octubre de 1992.
El art. 18.2 establece: "Las disposiciones de creación o modificación de los ficheros deberán indicar:
a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero automatizado y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal que, en su caso, se prevean.
f) Los órganos de la Administración responsables del fichero automatizado.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación y cancelación."

[204] El art. 24.2 de la LORTAD establece: " Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad y las cesiones de datos de carácter personal que se prevean realizar."

ro, la dirección del mismo y el número de ficheros que maneja o utiliza. ¿ Y el resto de las menciones ?, ¿ y la indicación de la finalidad ?, ¿ y la determinación del tipo de datos que son objeto de tratamiento ?. Sobre estos extremos nada. Estas omisiones y deficiencias, han sido corregidas en la nueva edición del Catálogo de ficheros 1997, donde, ya sí, se recogen todas las menciones exigidas por la ley, así como otras informaciones ciertamente interesantes para los estudiosos de estas cuestiones [205].

Pero no todo es un camino de rosas. Determinadas disfuncionalidades e intentos de soslayar la normativa protectora son más que el reflejo de la ignorancia y la superficialidad con que en algunos ámbitos se abordan estas cuestiones capitales. Por desgracia, parecen confirmarse los recelos apuntados por algún sector de la doctrina [206].

5.2.2. El Consentimiento del Afectado.

El consentimiento del sujeto constituye un elemento que, en principio, elimina el carácter ilícito de un ataque a un bien de la personalidad [207]. En materia de protección de datos personales, el consentimiento del afectado constituye un elemento indispensable, que justifica el tratamiento de datos personales por el responsable del fichero. Se erige, como señala Lucas Murillo de la Cueva, en la piedra angular a partir de la cual se construye el sistema de protección de datos personales frente al uso de la informática [208].

El consentimiento se revela como un poderoso elemento para afirmar la identidad de las personas, conforme a uno de los fines asignados a la legislación de protección de datos: la protección de la persona respecto al tratamiento automatizado de informaciones nominativas [209].

Como regla general, las legislaciones de protección de datos exigen, salvo excepciones expresamente tasadas en su articulado, el consentimiento previo del interesado para proceder a un tratamiento automatizado de sus datos personales.

Ahora bien, la noción de "consentimiento" aquí utilizada equivale a la de "consentimiento libre e informado": Libre, en cuanto otorgado al márgen de cualquier

[205] Catálogo de Ficheros 1997. Registro General de Protección de Datos. (CD).
[206] Vid. CASCAJO CASTRO, J.L., "Tratamiento automatizado de los datos de carácter personal", en la obra colectiva, edic. a cargo de J.M. Sauca, *Problemas actuales de los derechos fundamentales*, Universidad Carlos III & Boletín Oficial del Estado, Madrid, 1994, pp. 363-376; PEREZ LUÑO, A.E., "Comentario legislativo: la LORTAD...", cit., p. 419.
[207] Cfr. RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, cit., p. 334.
[208] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, cit., p. 61.
[209] Cfr. KAYSER, P., *La protection de la vie privée*, cit., p. 368.

presión o coacción física o psíquica; informado, como acabamos de señalar, para que el interesado pueda sopesar los riesgos y ventajas del tratamiento de sus datos y ejercer los derechos que le asisten.

La prestación del consentimiento no debe imponerse, por razones prácticas, mediante su formalización por escrito. Sin embargo, si deberá ser expreso y específico; es decir, debe ser referido al tratamiento de los datos referentes a su persona por el responsable del fichero y para una determinada finalidad. Además, deberá precisarse que tipos de datos, formas de tratamiento y, en su caso, transferencias o cesiones de datos a terceros, se autorizan. No caben, en consecuencia, autorizaciones generales, si no pronunciamientos caso por caso en los que el control pueda ejercerse de manera efectiva [210].

No obstante, si será preciso el consentimiento expreso y por escrito cuando del tratamiento de "datos sensibles" estemos hablando; así como de aquellos supuestos en los que de la prestación del consentimiento se deriven para el afectado cualquier género de carga o de gravamen.

El interesado debe tener también la posibilidad de revocar en cualquier momento su consentimiento. Ahora bien, la revocación no puede tener efectos retroactivos, ya que de lo contrario, resultaría ilegal de manera sobrevenida un tratamiento de datos personales previamente lícito.

5.2.3. Derecho de Acceso.

El derecho de acceso es una de las piezas esenciales de las legislaciones de protección de datos. Consiste en la facultad que se le concede al afectado de comprobar si se dispone de información sobre uno mismo, y conocer el origen del que procede la existencia de los datos, así como la finalidad con que se conserva [211].

Conocido el hecho de que figura en un fichero, los particulares pueden asimismo obtener comunicación en manera inteligible de las informaciones que le afectan.

Este conocimiento, no obstante, no presenta un carácter global y completo. Las legislaciones de protección de datos, o bien establecen el secreto absoluto sobre ciertas informaciones, o bien hacer primar determinados intereses sobre el ejercicio del derecho de acceso [212].

[210] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, cit., p. 59.
[211] Cfr. LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, cit., p. 187; *ID, Informática y protección de los datos personales*, cit., p. 75; OROZCO PARDO, G., "Consideraciones sobre los derechos de acceso y rectificación", cit., pp. 209-ss.
[212] Cfr. KNAPP, B., "La protection des données personnelles. Droit Public Suisse", en *Revue Internationale de Droit Comparé*, núm. 3, juillet-septembre 1982, p. 598.

La información que se obtendrá tras el ejercicio del derecho de acceso versará, cuanto menos, sobre los datos, las personas autorizadas a conocerlos, así como sobre la finalidad de los ficheros. Igualmente, ha de incluir las cesiones que se han hecho de los datos del afectado a terceros, así como la identidad de los cesionarios y la finalidad que éste persigue [213]. Como contrapartida, no parece incluirse dentro de su ámbito la obligación de comunicar las fuentes de información, ni el origen de las investigaciones de las informaciones.

Respecto a las personas legitimadas para ejercitar el derecho de acceso, y ante el silencio de la legislación protectora, éste parece configurarse como un derecho personalísimo, que no puede ejercitarse más que por su titular; el mandato no podría utilizarse más que para los declarados como incapaces [214]. Ello implica que no podrán ejercitarlo, ni el cónyuge, ni los herederos de la persona concernida, que son considerados como terceros respecto al acceso a los datos. Estas personas sólo podrían ser informadas tras el fallecimiento del titular del derecho de acceso y solamente en la medida en que demostraran un interés particularmente digno de protección para conocer estas informaciones. En todo caso no podrían acceder a informaciones referentes a terceras personas o versar sobre cuestiones tocantes a la esfera personalísima del titular del derecho.

Por otra parte, el derecho de acceso debe ser fácil de ejercitar, y los datos deben ser comunicados en un plazo razonable. Normalmente, debería producirse de manera inmediata el acceso y la comunicación de los datos; y en su defecto, dentro de un plazo razonable, computado desde la recepción de la petición de acceso. La naturaleza del tratamiento y los criterios organizativos del fichero determinarán el marco temporal en que deberá darse cumplida respuesta al derecho de acceso.

El derecho de acceso y la comunicación de las informaciones debería ejercitarse de manera gratuita. A este respecto, podrían crearse por los responsables de los ficheros, tanto públicos como privados, unas "secciones o departamentos de información", encargados de posibilitar a los interesados el ejercicio gratuito, y de manera clara, completa y exacta de su derecho de acceso.

No obstante, la mayor parte de las legislaciones del Derecho comparado prevén el establecimiento de un canon o contraprestación por ese acceso e información, que en ningún caso deberá ser excesivo, ni superior al coste real. Se trata de evitar con ello que ante unos elevados costes para el ejercicio de este derecho, se produjera una desigualdad entre los titulares de los mismos. De lo contrario, sólo aquéllos que dispusieran de medios económicos suficientes para hacer frente a tal remuneración podrían ejercitar su derecho de acceso, quedando los demás desamparados y desprotegidos.

[213] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos*, cit., p. 75.
[214] Cfr. ANCEL, P., "La protection des données personnelles. Aspects de Droit Privé Français", en *Revue Internationale de Droit Comparé*, núm. 3, juillet-septembre 1987, p. 621.

5.2.4. Derecho de Rectificación.

Si conocidos los datos que le afectan contenidos en ficheros, el individuo constata que aquéllos contienen errores, puede demandar la rectificación.

Este derecho se dirige a obtener la corrección o integración de aquellos datos que figuren de manera inexacta o incompleta en un fichero; también a actualizar la información obsoleta o desfasada [215]. Dos modalidades fundamentales cabe, pues, incluir en este derecho: 1. Sustitución. Cambio de los datos inexactos por datos correctos; 2. Complementación. Integración de los datos incompletos con informaciones complementarias que nos permiten obtener una visión adecuada a la realidad.

La cuestión esencial radica en saber, ante todo, a quien corresponde la carga de la prueba de la inexactitud u obsolecencia de los datos. Parece que normalmente el hecho de que un dato sea incorrecto deberá ser probado por la persona interesada. Parece que un tal "reparto de la prueba" es coherente con la regla general según la cual, el que prevaliéndose de un hecho pretenda tener un derecho debe demostrarlo [216]. Todo ello sin olvidar que este derecho no es más que la otra cara de la moneda del principio de calidad de los datos, que debiendo ser escrupulosamente respetado por todos los responsables de ficheros, impone a éstos la obligación de velar por la exactitud, actualidad y veracidad de los datos.

El "nuevo suministro" de datos que supone la rectificación, no debe suponer en ningún caso un menoscabo de los derechos de los ciudadanos. Sustituidos los datos incorrectos o incompletos, éstos deben ser borrados, para evitar que esa dualidad en el registro ocasione perjuicios a los individuos.

Respecto al momento de ejercicio de este derecho, consideramos que debe operar desde el momento mismo en que son recogidos en un fichero, independientemente de si han comenzado o no a ser tratados. Lo contrario significaría que el derecho de rectificación no estaría abierto a las personas interesadas más que a partir del momento en que los datos han sido "tratados", lo que excluiría la posibilidad de actuar contra ficheros, automatizados o no, que no han sido todavía objeto de un tratamiento automatizado [217].

Por otro lado, el responsable del fichero tendrá la obligación de hacer efectivo este derecho dentro de un plazo razonable, y sin coste alguno para el ciudadano [218]. La razón es lógica. El mantenimiento de datos inexactos o incorrectos durante un

[215] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, cit., p. 77.
[216] Cfr. KNAPP, B., "La protection des données personnelles. Droit Public Suisse", cit., p. 600.
[217] Cfr. FOCSANEANU, L., "La protection des données à caractère personnel...", cit., p. 89.
[218] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, cit., p. 78.

largo período de tiempo, puede acarrear graves consecuencias para los ciudadanos, a la vez que impediría al responsable del fichero la consecución de la finalidad perseguida con el registro de los datos. En relación a los costes, el ciudadano no puede ser sometido al pago de un canon o gravamen por el ejercicio de un derecho que le es inherentes; y además para rectificar una situación de la que no es en absoluto responsable, si no generalmente víctima.

Cuando los datos hayan sido cedidos a terceros, y para proteger de manera consecuente los intereses del afectado, el responsable del fichero deberá comunicar a aquéllos la rectificación de los datos, con objeto de que puedan rectificar o completar a su vez los datos en cuestión.

5.2.5. Derecho de Cancelación.

Si como consecuencia del ejercicio del derecho de acceso el titular de los datos personales constata que los datos que obran en el fichero no son pertinentes o adecuados en relación con la finalidad para la que fueron registrados, o pertenecen a una categoría tal que impide su registro, o se ha procedido a su registro de una forma ilegal o contraviniendo el consentimiento del interesado, podrá ejercitar su derecho de cancelación para eliminar del fichero aquellos datos personales [219].

Resulta obvio, por tanto, como deberá procederse a la cancelación de aquellos datos personales que consten en ficheros contraviniendo, en el ámbito material, los principios de protección de datos antes apuntados; y en el ámbito subjetivo, el consentimiento libre e informado del sujeto, que constituye, salvo excepciones legalmente establecidas, el único título habilitante para el tratamiento automatizado de datos personales.

Ahora bien, el nudo gordiano de este derecho estriba en determinar que deba entenderse por "cancelación". La casi totalidad de leyes de protección de datos hacen referencia a una operación jurídica tendente a eliminar, a borrar los datos existentes en ficheros informatizados a instancia de las personas interesadas [220]. La cuestión a dilucidar es si la cancelación debe equivaler a la destrucción material o borrado de los datos, o debe limitarse simplemente al apartamiento de tales datos de los canales de uso, señalando que no pueden ser utilizados, pero conservándolos en el propio fichero. Creemos que la propia naturaleza y objetivos de

[219] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, cit., p. 79; OROZCO PARDO, G., "Los derechos de la persona en la LORTAD", en *Informática y Derecho*, núms. 6-7, 1994, pp. 151-201.

[220] Cfr. ARROYO YANES, L.M., "La cancelación de datos personales en ficheros de titularidad pública en el proyecto de la LORTAD", en *Actas del III Congreso Iberoamericano de Informática y Derecho* (Mérida, septiembre 1992), publicadas en *Informática y Derecho*, núm. 4, 1994, pp. 181-200.

este derecho nos llevan a asumir la primera de las variables. Los derechos de los ciudadanos ante un uso ilegítimo de sus datos personales sólo pueden salvaguardarse si se eliminan totalmente la causa que puede dar lugar a eventuales perjuicios. Además, ¿ que sentido tendría conservar unos datos incorrectos ?, ¿ no podría darse lugar a una "tentación futura" y utilizar los datos incorrectos o ilegítimos de una manera torticera ?.

Respecto al plazo en que deba operarse la cancelación, siguiendo a Lucas Murillo de la Cueva, debe considerarse que transcurrido el que contemplaba la autorización del afectado, o la disposición normativa que habilitaba para su recogida [221]. La cancelación deberá también operarse cuando, cumplida la finalidad para la que los datos fueron registrados, éstos dejan de ser relevantes para el titular del fichero. Igual tratamiento debe otorgarse si, establecida una determina finalidad, se constata la posibilidad de verificarla en un plazo razonable. El principio de conservación limitada de los datos encuentra aquí una de sus manifestaciones.

Los responsables de ficheros, al igual que lo señalado anteriormente para el derecho de rectificación, deben proceder a la cancelación de oficio de aquellos datos que consten indebidamente en su fichero. Si constatada por el titular de los datos la "impertinencia" de las informaciones que constan en un fichero, debe el responsable proceder, a su requerimiento, de manera inmediata y gratuita a su cancelación.

Si los datos hubieran sido cedidos a terceros, el responsable de la cesión deberá comunicar a los cesionarios la cancelación de los datos, para que puedan éstos a su vez proceder a la cancelación de los datos en cuestión.

5.2.6. Derecho de Oposición del interesado. La impugnación de las decisiones individuales automatizadas.

Los ciudadanos tienen derecho a oponerse por motivos legítimos a que los datos personales que les conciernen sean objeto de tratamiento. Entre los motivos legítimos puede citarse la falta de justificación legal de un tratamiento determinado de datos personales. A *sensu contrario*, la mayoría de las legislaciones nacionales establecen la imposibilidad de oponerse cuando de un tratamiento lícito y necesario para el cumplimiento de determinadas tareas, públicas o privadas, se trate.

Estas habilitaciones legales, de contornos a propósito difusos, tienden a establecer un equilibrio entre el reconocimiento a las personas físicas de un derecho sobre las informaciones que le conciernen, y el poder, generalmente de la autoridad pública, para registrar y tratar estas informaciones. Pero, como indica Kayser,

[221] Cfr. LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, cit., p. 80.

la realización de este equilibrio se revela difícil en lo que respecta a los tratamientos, las informaciones y las razones que posibilitan el ejercicio de este derecho [222].

Se plantean varios problemas. En primer lugar, que sentido deba darse a la noción de "motivos legítimos". En segundo lugar, que deba entenderse por "tratamiento lícito y necesario". Respecto a esta última cuestión, parece más interesante que establecer unos criterios enumerativos de situaciones en las que el tratamiento se atemperará a esas coordenadas, el señalamiento explícito, con respeto de la seguridad jurídica, de la imposibilidad de oposición en el acto legal o reglamentario habilitador del tratamiento.

No obstante estas objeciones, debe garantizarse a todo ciudadano el efectivo ejercicio de este derecho de oposición, como manifestación de sus posibilidades de autodeterminación personal en el seno de las sociedades democráticas.

Ahora bien, si este derecho debe garantizarse en el sector público, donde debe cobrar especial relevancia, vigencia y efectividad es en el ámbito del sector privado. Y ello es así por la proliferación de empresas dedicadas al "tráfico" de datos personales relativos a todo género de situaciones y circunstancias.

Lo primero que sorprende de estos "mercaderes de la información" es la absoluta libertad e impunidad con que operan. Algunos, no satisfechos con ello, incluso se anuncian públicamente. Alentados por toda una pléyade de empresarios, por llamarles de alguna forma correcta, y respaldados por un amplio elenco de "chivatos informáticos", aumentan constantemente sus ya de por sí grandes bases de datos y se infiltran en todos los sectores.

A esta situación alarmante conviene poner freno de una manera inmediata y radical. No puede tolerarse el lucro de gente sin escrúpulos a costa de los derechos y la honorabilidad de las personas.

La solución lógica y coherente sería la prohibición a estas entidades de dedicarse a tales actividades sin un control legal previo y concienzudo. Una vez establecida esta habilitación legal, debería procederse a un riguroso control sobre sus "fuentes de aprovisionamiento" de datos, que en ningún caso deberá menoscabar el consentimiento e información del afectado. Todo ello teniendo como marco general la presunción *iuris tantum* de que ningún ciudadano desea recibir informaciones, comunicaciones o datos no solicitados.

La situación real difiere, no obstante, de manera radical con estas previsiones. Como ha denunciado Pérez Luño, así se alude hoy a los denominados "ficheros Robinson" para referirse a aquellos ficheros en los que deberían inscribirse los ciudadanos que no quieran ver menoscabados su derechos por la recepción de

[222] Cfr. KAYSER, P., *La protection de la vie privée,* cit., p. 350.

propaganda no solicitada ni deseada. Es decir, se consagra la obligación para los ciudadanos de inscribirse en un archivo de datos para que sean respetados sus derechos y libertades, en lugar de hacer recaer en las empresas que comercializan los datos la prueba de que existe un consentimiento previo de cuantas personas figuran en sus bases de datos de información comercial [223].

En el caso de que la oposición del interesado se manifestara, el responsable del tratamiento deberá suspender *ipso facto* el tratamiento de los datos personales. Si pese a esta oposición, el tratamiento tuviera lugar, deberá reconocerse al interesado la posibilidad de plantear una acción tendente a la reparación de las consecuencias que dicho tratamiento ilícito le hubiera acarreado (por ejemplo, la anulación de las decisiones tomadas sobre la base del tratamiento de datos). Si el tratamiento estuviera en trámite de ejecución, o existiera el riesgo de que un tratamiento tal pudiera verificarse, el interesado deberá poder ejercitar una acción tendente a la paralización y/o cesación del tratamiento abusivo que le perturba [224].

Establecida la necesidad de garantizar a los ciudadanos un derecho de oposición frente a un tratamiento automatizado de sus datos personales, conviene también plantearse la posibilidad de impugnación de aquellas decisiones que, tomando como base una serie de informaciones dispersas sobre nuestras actitudes, gustos, apetencias y demás indicaciones de nuestra personalidad, impliquen una valoración de su comportamiento personal cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal.

La utilización abusiva de la informática en la toma de decisiones constituye uno de los riesgos esenciales que se plantean en el futuro, ya que el resultado que proporciona la "máquina", que utiliza cada día programas más refinados, e incluso sistemas expertos, tiene un carácter aparentemente objetivo e incontestable, al que el responsable de tomar la decisión puede conceder una importancia decisiva. Por todo ello, debe consagrarse la idea según la cual las personas tendrán el derecho a no verse sometida a una decisión administrativa o privada que les resulte perjudicial y que se base exclusivamente en un tratamiento automatizado que dé un perfil de su personalidad. Tres circunstancias, por tanto, deben concurrir para que pueda articularse tal oposición:

a. La persona debe estar sometida a una decisión que le resulte perjudicial. Debe tratarse de una decisión a la que pueda oponerse, que comporte consecuencias a su respecto.
b. Debe tratarse de una decisión basada exclusivamente en un tratamiento automatizado. La informática puede servir de ayuda a la decisión, pero no

[223] Cfr. PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho y Constitución,* cit., pp. 376-378; ID, "Comentario legislativo : La LORTAD y los derechos fundamentales", cit., pp. 416-419.
[224] Cfr. KNAPP, B., "La protection des données personnelles...", cit., p. 601.

constituir en ningún caso su única base, debiendo dejarse a la apreciación humana el lugar que le corresponde.

c. El tratamiento debe atribuir a los datos relativos al interesado variables que permitan determinar un perfil de personalidad tipo, considerado bueno o malo. Parecen excluirse así aquellos casos en los que el sistema no define el perfil de la personalidad, tal como el supuesto de que una persona no pueda obtener el importe solicitado de un cajero automático, por que haya superado su crédito

5.3. *La proteccion de los "datos sensibles".*

5.3.1. Conceptuación de los datos sensibles.

Los datos personales, si por un lado pueden ser agrupados en una categoría homogénea, por otro, se prestan a ser reconsiderados de acuerdo con la diversa disciplina a la que está sometida su circulación. Una reconsideración respecto a la categoría general lo constituyen, precisamente, los datos sensibles. No existe un acuerdo unánime ni en la doctrina ni en el derecho comparado acerca de que sean o que deba entenderse por datos sensibles. Lo que si parece existir es un acuerdo casi generalizado, en su abstracción, respecto a la necesidad de una regulación diferenciada respecto a ciertos datos personales cuyas peculiaridades exigen formas de tutela particulares.

Es precisamente en la determinación de esas notas distintivas donde surgen las discrepancias.

Pérez Luño considera como tales aquellos que tienen una inmediata incidencia en la privacidad o un riesgo para practicas discriminatorias. También considera como tales aquellas informaciones que hacen referencia a convicciones personales, así como las referentes inmediatamente al resto de las libertades [225].

Toniatti por su parte, establece una doble consideración respecto a la conceptualización de los datos sensibles:

— Criterio Formal: Aquellos datos que presentan algunos requisitos reforzados para que limitan su libre adquisición, circulación, etc.
— Criterio Material: Cualificados por su afectación a una esfera íntima subjetiva de particular delicadeza. Aquellos que más directamente se refieren ya a la esfera personal e íntima ya a la titularidad de los derechos fundamentales de libertad [226].

[225] Cfr. PEREZ LUÑO, A.E., *Libertad informática y leyes de protección de datos personales*, cit., p. 152; ID., "Comentario Legislativo. La LORTAD y los derechos fundamentales", en *Derechos y Libertades*, núm. 1, febrero-octubre 1993, p. 406.
[226] Cfr. TONIATTI, R., "Libertad Informática y Derecho a la protección de los Datos Personales...", cit., p. 155.

Madrid Conesa, por último, estructura la consideración de los datos sensibles en torno a dos variables:

a. Aquellos cuyo tratamiento incorpora peligros de discriminación.
b. Aquellos que son irrelevantes desde el punto de vista de las relaciones externas de los ciudadanos; es decir, aquellos más directamente conectados con el ámbito más personal e íntimo [227].

Esta breve semblanza doctrinal nos ilustra respecto a lo que venimos señalando respecto a que deba entenderse por datos sensibles. Lo cierto es que, pese a todas las diferencias, existe un acuerdo respecto a una especial tutela, protección y garantías para estos datos.

Los datos sensibles, como cualesquiera otros datos, no pueden ser considerados estáticamente, sino en el proceso general de tratamiento automatizado del que constituyen su objeto, e incluso su fin. Surge aquí plantearse pues el carácter dinámico de su determinación.

5.3.2. Determinación de los datos sensibles: su dinamicidad.

Dejando al margen la importancia que reviste la protección de ciertas categorías de datos que por su propia naturaleza pueden poner en peligro la intimidad de los ciudadanos, asistimos a un consenso casi generalizado respecto a la consideración de que no es la naturaleza de los datos la que atenta contra el derecho a la intimidad, sino el concreto contexto en el que se efectúa el tratamiento de dichos datos [228].

No es la clasificación abstracta de un dato como más o menos cercano al ámbito de las personas, ni la determinación de que por su naturaleza tiene carácter de secreto o no lo que determina su tutela, sino el ámbito concreto de su uso [229].

La tutela de las informaciones no puede ya quedar limitada a aquellas de cuya calidad así se exija, en una visión estática, sino que debe extenderse a la dinámica de su uso o funcionalidad. Es evidente, como señala el Pérez Luño, que cualquier información, en principio neutra e irrelevante, puede convertirse en sensible a tenor del uso que se haga de las mismas [230].

[227] Cfr. MADRID CONESA, F., *Derecho a la Intimidad, Informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984, p. 88.
[228] En este sentido se expresa la Comunidad Europea. Vid. sobre ello: 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, DOCE Nº L 281, 23.11.1995, especialmente sus Considerandos 33-36 y su art. 8.
[229] Cfr. DENNINGER, E., "El derecho a la autodeterminación informativa", cit., p. 273.
[230] Cfr. PEREZ LUÑO, A.E., Comentario Legislativo: La LORTAD y los derechos fundamentales", cit., p. 413.

Existe la posibilidad, como venimos señalando, que datos *a priori* irrelevantes desde la consideración de la privacidad de las personas, sin embargo, en conexión con otros datos puedan servir para hacer completamente diáfana y transparente la personalidad de los ciudadanos.

Se aboga así por un sistema dinámico en la protección de los datos sensibles. La experiencia del Derecho Comparado, remisa a una amplia enumeración de la categoría de los datos sensibles, y su encorsetamiento en rígidas normas legales, nos dan una muestra de cuan inoperantes pueden ser las declaraciones grandilocuentes, paralelamente vacías de garantías.

Será el devenir de los tiempos, y el consecuente cambio en las estructuras sociales, el que determinará la inclusión o no de determinados datos en la categoría de "sensibles", y por lo tanto su acomodación a la realidad fáctica de su tratamiento.

Tiempo y espacio se revelan aquí como variables ineludibles de un verdadero y efectivo sistema de garantías.

No obstante, no todo será variabilidad, acomodación; si no que pese a las circunstancias cambiantes, siempre habrá un mínimo de "sensibilidad" que nos indicará el norte a seguir, y nos permitirá, alejándonos de la niebla, conocer ese mínimo irreductible que para el ser humano constituye su dignidad.

5.3.3. ¿Numerus Clausus o Numerus Apertus?.

El carácter dinámico que venimos propugnando en la determinación de los datos sensibles, nos lleva a plantearnos cual debe ser la formula o método a través del cual deben positivizarse, y por lo tanto, determinarse su régimen específico y peculiar.

El decantamiento por una opción de numerus clausus o numerus apertus, dependerá, no tanto de la sensibilidad del legislador o de su mayor amplitud de miras, sino que lo realmente determinante será la concepción que se comparta acerca de la amplitud del bien jurídico protegido, bien limitado a la concepción individualista de la intimidad, o bien, además del anterior, al ejercicio efectivo del resto de las libertades. Por que como señala Madrid Conesa, el problema del derecho a la intimidad se resuelve, en última instancia, en un problema de libertad [231].

Por razones de seguridad jurídica es cierto que deberá procederse a la determinación legal de aquellos supuestos subsumibles bajo el ámbito de los datos sensibles. Ahora bien, será necesaria la utilización de cláusulas abiertas o generales, lo

[231] Cfr. MADRID CONESA, F., *Derecho a la Intimidad, Informática y Estado de Derecho,* cit., p. 45.

suficientemente precisas, en su vaguedad, como para determinar su ámbito de aplicación; pero, lo suficientemente amplias como para permitir la modelación en la conceptuación de los datos de acuerdo a las exigencias que demande el efectivo cumplimiento y garantía de los derechos de los ciudadanos.

Pasemos a ver algunos ejemplos de "determinación legislativa" de los datos sensibles.

Según la Convención Europea los datos sensibles (art. 6) son *"los datos de carácter personal que revelaren el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual... y los referentes a las condenas criminales"* [232].

Las Comunidades Europeas enumeran como tales *"los datos que revelen el origen racial y étnico, la opinión política, las convicciones religiosas, filosóficas o morales, la afiliación sindical, así como las informaciones relacionadas con la salud y la vida sexual"* [233].

La Ley francesa (art. 31) incluye en esta categoría *"los datos nominativos que directa o indirectamente hagan constar los orígenes raciales o las opiniones políticas, filosóficas, religiosas o la afiliación sindical de las personas"*.

En Gran Bretaña se incluyen (art. 2.3 de la *Data Protection Act*) *"los datos relativos al origen racial, a las opiniones políticas, religiosas o de otra naturaleza, a la salud física y mental, a la vida sexual y a las condenas penales"*.

En Suiza, la ley define los datos sensibles como *"los datos personales acerca de las opiniones o actividades religiosas, filosóficas, políticas o sindicales, la salud, la esfera íntima o la pertenencia a una raza, medidas de asistencia social, investigaciones o sanciones penales o administrativas y el perfil de la personalidad, como un conjunto de datos que permite apreciar las características esenciales de la personalidad de una persona física"* [234].

Como se puede observar las categorías recogidas son casi idénticas, si exceptuamos las relativas a las condenas penales, cuya inclusión o no se debe a la diferente perspectiva con que los ordenamientos nacionales entienden la publicidad de las actuaciones penales y el régimen de los datos tratados o generados en tales actuaciones.

[232] *Protección de datos. Convenio del Consejo de Europa de 1981,* cit., pp. 33-34.

[233] Art. 8 de la Directiva del Parlamento y del Consejo relativa a la protección de las personas físicas..., cit.

[234] Cfr. MONTAVON, P., "De la confidentialité des donnes personnelles au sein des enterprises", en la obra colectiva La protection de la personalité. Bilan et perspectives d´un nouveau droit, Editions Universitaires Fribourg Suisse, Fribourg, 1993, p. 80.

Conviene tener en consideración, que no será la enumeración de los datos la que determinará su efectivo régimen de garantías, sino la amplitud de supuestos que puedan incluirse bajo su enumeración lineal. Es decir, se trata de un problema de interpretación acerca de que debe entenderse bajo las dicciones legales de datos sensibles.

5.3.4. Régimen jurídico de los datos sensibles.

Entre las muchas consideraciones hechas sobre las legislaciones de protección de los datos personales cabe destacar positivamente el hecho de que la mayoría de ellas incluye en su articulado un apartado específico dedicado a la regulación de los datos sensibles, otorgándole una protección reforzada.

Para esta categoría de datos el principio general, es al contrario del existente para los datos ordinarios, el de la prohibición de recogida y tratamiento excepto en los casos previsto por la ley.

Desde el punto de vista del afectado el elemento del consentimiento se revela como fundamental para proceder a un tratamiento de datos personales de tal etiología, como expresión máxima y global de su derecho a la autodeterminación informativa.

Pero no debe tratarse de un consentimiento simple, sino de un *"consentimiento informado"*, a fin de que el interesado pueda sopesar los riesgos y ventajas del tratamiento de sus datos sensibles y ejercer los derechos recogidos en la norma.

El consentimiento de la persona concernida acerca del tratamiento de sus datos sensibles se constituye, así, como elemento fundamental articulador del sistema de garantías.

Será el consentimiento, y sus diferentes manifestaciones, el que determinará la posibilidad de tratamiento automatizado de estos datos.

Ahora bien, dos objeciones fundamentales cabe hacer a la mayor parte de las previsiones legislativas sobre esta cuestión:

a. Establecimiento de una parca regulación, consolidándose así un sistema de *numerus clausus*. No es esta afirmación contradictoria con la sostenida *supra* acerca de la necesidad de una generalidad en la dicción legal de los supuestos considerados como datos sensibles. Las soluciones legislativas parecen considerarlos datos sensibles en función de una tutela estática, que presenta como referente fundamental el derecho a la intimidad, cuya salvaguarda se propone llevar a efecto. Se consigue con ello sólo una solución parcial del problema.

b. Alusión a conceptos jurídicos ciertamente indeterminados, que no pueden considerarse como generales, en la postura que venimos defendiendo, sino ciertamente como ambiguos y que producen en el momento de su alegación por algún ciudadano afectado, graves problemas de interpretación respecto al alcance de su contenido. Procederemos por ello a intentar dar una visión lo más completa posible acerca de que supuestos son, a nuestro criterio, subsumibles bajo las expresiones legales contenidas en las legislaciones de protección de datos.

b.a. Ideología. Deberá incluir tanto las opiniones políticas, como las referentes a la afiliación sindical. Se englobarán las informaciones del interesado sobre sus actividades en el terreno político y sindical. Respecto a las informaciones referentes a la pertenencia a un sindicato nos adherimos a aquellos países que en sus legislaciones consideran que las informaciones referentes a la pertenencia a un sindicato llevan consigo riesgos para la intimidad personal.
Considerando la objeción que podría plantearsenos respecto al requisito suplementario de la afiliación, en el ámbito sindical, recogido entre otras legislaciones por la Comunidad Europea, hacemos notar nuestra oposición a tal requisito suplementario. El conocimiento de las opiniones políticas tiene también su principal baluarte en la afiliación de los ciudadanos a los partidos políticos o en el desarrollo de actividades de apoyo, generalmente bajo la atenta mirada de los órganos rectores de los mismos. Así pues sólo quedan dos alternativas, o bien se prescinde en ambos casos del requisito de la afiliación como elemento delimitador de la adscripción a una determinada opción política o sindical, o bien, se exige en ambos casos, con el riesgo evidente de limitación del ámbito material protegido [235].

b.b. Religión y Creencias. Se considerarán como tales las creencias religiosas, convicciones filosóficas y morales, incluida la falta de creencias religiosas, así como las informaciones relativas a las actividades del interesado en el terreno religioso o filosófico, y las actividades o actitudes que se deriven de tales creencias o convicciones. Las creencias no religiosas o no filosóficas también deben constituir datos especiales.

b.c. Origen racial. Comprende los datos o informaciones relativos a la pertenencia a una etnia, pueblo o nación, al margen de su adscripción a un determinado Estado. Deberá incluirse asimismo la información sobre el color de la piel.

b.d. Salud. Los datos personales relativos a la salud pueden catalogarse, como hace *Toniatti*, de supersensibles [236].

[235] Cfr. *Protección de datos. Convenio del Consejo de Europa*, cit., p. 33. Asimismo, Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas, cit.

[236] Cfr. TONIATTI, R., "Libertad Informática y Derecho a la Protección de los Datos Personales: Principios de Legislación Comparada", cit., pp. 158-ss.

Conciernen a un ámbito merecedor de información reforzada hasta el punto de excluir normalmente el acceso directo de los individuos a los propios datos personales [237]. Abarca las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. Pueden tratarse de datos referentes a un individuo de buena salud, enfermo o fallecido. Estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas. Deben hacerse, no obstante, dos consideraciones respecto a este tipo de datos:

1. Habrá que tener especial cuidado respecto a los datos referentes a la salud mental en el futuro, pues se corre el riesgo de hacer ingresar a los afectados en una especie de "censos negros", con el paralelo peligro para el ejercicio de sus derechos. Se puede así proceder al tratamiento de estos datos sensibles basándose en meras sospechas que no presenten ninguna constatación real. Serán las verdaderas necesidades del tratamiento médico y la evolución de la enfermedad, junto a unas razonables previsiones de futuro, las que deben determinar la inclusión de estos datos.
2. Respecto a las referencias al alcohol y a las drogas, deberán establecerse límites flexibles, atemperados a los efectos particulares sobre el individuo concreto. Máxime cuando no está claro ni para el Derecho Penal, ni para la ciencia toxicológica, donde están los límites entre el consumo, uso y abuso de drogas o alcohol. La estricta referencia al término drogas engloba otras sustancias perjudiciales para la salud, tales como los estupefacientes y los psicotrópicos.

b.e. Vida Sexual. Es este un término ciertamente relativo y estrictamente personal. Como señala el Prof. López Ibor "la conducta sexual relativa al objetivo que la motiva puede ser influida por los actos positivos o negativos referentes a la finalidad de lo sexual en sí. Por lo tanto varía notablemente según los individuos, desplazándose desde el mismo acto sexual a sus elementos y derivados más o menos remotos" [238].
Deberán incluirse por lo tanto todos los datos relativos a la actividad sexual de los ciudadanos, así como la ausencia de dicha actividad, y las consecuencias que de ellas se derivan.
Se considerarán también como tales los datos de "referencia indirecta", es decir aquellos de los que puedan extraerse ciertos datos indiciarios de su conducta sexual, tales como suscripción a revistas de contenido erótico, anuncios de contactos, pertenencia a ciertos colectivos de defensa de homosexuales o/y lesbianas, etc.

b.f. Infracciones penales o administrativas. Debe partirse de la incorrecta denominación empleada por el legislador español para hacer referencia a estos datos. Debería haber empleado más bien el de *condenas*, por cuanto que son las sentencias en las que éstas se establecen las que incorporan una serie de datos que pueden menoscabar gravemente la intimidad de los ciudadanos. Si a ello unimos la conservación de datos referentes al cumplimiento de las mismas, una vez que dichas condenas han sido ya cumplidas o se han extinguido, el potencial lesivo es enorme.
Las mismas consideraciones caben, *mutatis mutandi*, respecto del empleo del término infracciones administrativas.
Por tales infracciones deberán entenderse las sanciones fundadas en una norma penal o administrativa e impuestas en el marco de un procedimiento penal o sancionador-administrativo.

[237] Sobre la política desarrollada en Francia y Gran Bretaña respecto al acceso a los datos médicos, especialmente de afectados por el SIDA, vid. TONIATTI, R., "Libertad informática y Derecho a la Protección de los Datos Personales...", cit., pp. 159-ss.
[238] Cfr. *El Libro de la Vida Sexual*, dirig. por J.J. López Ibor, Danae, Madrid, 1968, p. 410.

5.3.5. Excepciones a la prohibición de tratamiento de datos sensibles: La salvaguarda del "interés general".

El estudio del régimen jurídico de los datos sensibles quedaría incompleto si no recogiéramos también las excepciones que se establecen a la prohibición general de efectuar un tratamiento automatizado de datos sensibles. Es precisamente en las excepciones donde hay que mirar para ver cual es el efectivo sistema de protección y de garantías otorgado a los ciudadanos. Declarados rimbombantemente una serie de derechos, es habitual su derogación posterior de manera soterrada o encubierta, amparándose en ineludibles deberes del Estado, dando una imagen garantista al ciudadano, cuando realmente lo que se está configurando es un verdadero asalto a sus derechos y libertades.

En esta línea, la posibilidad de tratamiento automatizado de datos sensibles se tolera en los supuestos en que exista una habilitación legal por razones de interés general.

Las críticas apuntadas anteriormente se acentúan ante esta posibilidad, que presenta como único anclaje con la legalidad la abstracta e indeterminada referencia al interés general. Nada hace el legislador para colmar nuestras dudas. Sólo hay una cosa cierta, por esta vía se abre una puerta para el tratamiento de datos referentes a cuestiones tales como el origen racial, la salud y la vida sexual.

De nuevo se acude a conceptos jurídicos indeterminados, que lejos de aportar flexibilidad en su articulación, lo que hacen es atraer negros nubarrones sobre cual es el verdadero alcance de esta excepción. Se trata, como vemos, de una regulación fundada en un criterio restrictivo sobre la subsistencia de un derecho individual merecedor de protección que deja paso al prevalente interés nacional [239].

Será preciso determinar en este instante que se entiende por interés general.

[239] Cfr. TONIATTI, R., "Libertad Informática y Derecho a la protección de los Datos Personales...", cit., p. 157.

Siguiendo lo señalado por la Comisión de las Comunidades Europeas, pueden considerarse englobadas en tal denominación genérica todas aquellas medidas necesarias para la salvaguarda de los valores fundamentales de una sociedad democrática [240]. En idénticos términos se expresa el Consejo de Europa [241].

Pero la concurrencia de dicho interés general deberá hacerse constar mediante una Ley. Nada se suele afirmar acerca de cual deba ser el rango normativo de esta norma habilitante; cuestión ésta que queda diferida a las peculiaridades constitucionales y legislativas de cada uno de los Estados.

Ante esta falta de unificación regulativa conviene señalar que en dicha disposición legal deberán precisarse los datos que pueden ser tratados, las personas destinatarias de los mismos, la cualificación del responsable del tratamiento, las personas autorizadas a acceder a ellos, así como las garantías apropiadas contra los usos abusivos y los accesos no autorizados.

Sólo con estas menciones de la norma habilitante podrán salvarse las garantías que para los derechos de los ciudadanos establecen los Estados democráticos de Derecho.

Por último, conviene prestar una especial atención al tratamiento de datos sensibles efectuado por los Cuerpos de Seguridad del Estado para la prevención y represión de actividades delictivas.

Como señaló López Garrido, es claro que siempre la policía ha tenido en su poder ficheros. Pero se trataba de ficheros represivos. Quiere decirse que tales ficheros se confeccionaban después de que la persona fichada había sido considerada culpable de la comisión de un determinado delito. La introducción de ficheros automatizados en el desarrollo de las tareas policiales arroja una perspectiva ciertamente distinta. Se trata de ficheros que podemos considerar como preventivos; es decir, se establece primero aquella conducta que el individuo tendría que llevar a cabo y, sobre todo, se hace un verdadero "peinado" en la población de aquellos que pudieran en el futuro cometer tales conductas. Se trata de una acción preventiva que, como tal, tiene una dinámica de generalización, de exhaustividad casi ilimitadas e imparable [242].

Las circunstancias "objetivas" que determinan la posibilidad de dicho tratamiento son, generalmente, los fines de una investigación concreta. Este término debe incluirse dentro del marco más amplio de la *"represión de los delitos"*, y que comprendería tanto la investigación de los delitos como su persecución. Esta posibilidad, que pudiera parecer lógica como medio de salvaguarda de la *seguridad pública* [243], sin embargo adolece de tal carácter ante la total desarticulación del sistema de garantías de los ciudadanos.

[240] Cfr., Directiva del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas... cit., especialmente su Considerando nº 43 y su art. 13.

[241] Cfr. *Protección de datos. Convenio del Consejo de Europa de 1981*, cit., p. 36.

[242] Cfr. LOPEZ GARRIDO, D., "La sociedad informatizada y la crisis del Estado del bienestar", en *Revista de Estudios Políticos*, núm. 48, noviembre-diciembre 1985, pp. 27-45.

En la mayoría de los casos, por contra, se deja a los propios responsables del tratamiento la determinación "unilateral", de cuando los datos deberán ser utilizados, así como la amplitud material y temporal de dicha utilización. Difícilmente conocerá el afectado que se está procediendo a una utilización de sus datos sensibles por parte de las Fuerzas y Cuerpos de Seguridad. Además se exime a éstos de la concesión a los afectados de los derechos de acceso, rectificación y control. Esto parece ser, en su sin razón, lo más coherente. Si un ciudadano desconoce que sus datos sensibles están siendo objeto de tratamiento automatizado por parte de las Fuerzas y Cuerpos de Seguridad, difícilmente tendrá la "necesidad", por ese desconocimiento, de ejercitar las restantes facultades que configuran su derecho a la autodeterminación informativa.

Ante estas situaciones, el problema no estará tanto en la derogación de los derechos de los ciudadanos, como fundamentalmente en la consolidación de una potestad ciertamente arbitraria.

5.4. *La seguridad de la información.*

La seguridad de los sistemas de información constituye un elemento necesario en la sociedad moderna. Los modernos servicios de información electrónica exigen una infraestructura segura, con equipos y programas y seguros, y una utilización y gestión seguras.

Todo planteamiento relativo a la seguridad de la información tratada por medios electrónicos debe reflejar el deseo de cualquier sociedad de actuar con eficacia y a un tiempo protegiéndose en un mundo de rápidos cambios.

En los últimos años, las tecnologías de la información han pasado a ocupar un papel importante en casi todos los sectores sociales. Consecuentemente, los sistemas de seguridad de la información han devenido un componente esencial y omnipresente en la evolución sociopolítica y económica.

Es por ello, que los sistemas de seguridad de la información deben responder a tres exigencias ineludibles:

[243] En torno a la delimitación del concepto de seguridad pública, el Consejo de Europa, en la Memoria Explicativa, número 56, del Convenio 108 para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, establece que " la noción de seguridad del Estado deberá entenderse en el sentido tradicional de protección de la soberanía nacional contra amenazas internas o externas, incluida la protección de las relaciones internacionales del Estado", vid. sobre ello: *Protección de datos. Convenio del Consejo de Europa*, cit., p. 36.

— Confidencialidad: impedir la divulgación no autorizada de la información.
— Integridad: impedir la modificación no autorizada de la información.
— Disponibilidad: impedir la retención no autorizada de información o recursos [244].

Por lo que respecta a la protección de los datos personales, los riesgos para los derechos y libertades de los ciudadanos no se limitan al momento de la recogida, almacenamiento y transmisión; si no que también pueden proceder de un acceso no autorizado y/o un uso abusivo de los datos por parte de terceros. La seguridad, por tanto, debe tutelar el carácter secreto de los datos conocidos, y evitar el conocimiento, la manipulación o la supresión por parte de personas no autorizadas a efectuar su procesamiento [245]. Si la recogida, utilización o transmisión de datos de carácter personal están rodeadas en todas las legislaciones de una serie de garantías, éstas devienen inútiles si cualquiera puede penetrar en un fichero y tener acceso a tales datos.

Ahora bien, la seguridad es también una obligación inherente a todos los responsables de ficheros. Por ello, deben adoptar todas las medidas técnicas y de organización necesarias para proteger los datos del fichero contra el acceso no autorizado de terceros y contra la perdida accidental de datos, incluidos la destrucción accidental o no autorizada de datos, su modificación no autorizada o cualquier otro tipo de tratamiento autorizado.

La no adopción de estas medidas implicará la atribución de responsabilidad por los daños y perjuicios causados. Las personas que, de hecho o por convención con el responsable, controlen las operaciones relacionadas con el fichero de dato son responsables asimismo del cumplimiento de los requisitos de seguridad. Esta responsabilidad será dirigida, según proceda, tanto al responsable del fichero, como a las agencias de tratamiento de información que efectúen operaciones de tratamiento en nombre del responsable del fichero.

La determinación y exigencia de responsabilidades constituye, de este modo, una garantía importante e inexcusable para los ciudadanos y la defensa de sus derechos. De nada serviría que se nos garantizaran una serie de derechos si, por vía indirecta ("por la puerta de atrás"), los datos son accesibles, manipulables o destruibles por cualquiera. Las medidas de seguridad deben evitar, consecuentemente, que manifestaciones de nuestra vida personal o social sean accesibles con carácter general, se manipulen o, cuando nos sean favorables, se silencien. El daño para nuestra libertad, y sobre todo nuestra dignidad e identidad personales, puede ser enorme.

[244] Cfr. Decisión 92/242, de 31 de marzo de 1992, relativa a la seguridad de los sistemas de información, DOCE L 123, de 08.05.92.
[245] Cfr. FROSINI, V., "Banco de datos y tutela de la persona", en *Revista de Estudios Políticos*, núm. 30, noviembre-diciembre 1982, p. 36.

Respecto al alcance de las responsabilidades, no deben limitarse sólo a los daños y perjuicios materiales; si no que deben incluir también los daños y perjuicios morales.

Las medidas técnicas de seguridad incluirán medidas de seguridad relacionadas con el acceso a instalaciones de tratamiento y almacenamiento de datos, códigos de identificación para las personas autorizadas a entrar en dichas instalaciones, medidas de protección de la información (utilización de contraseñas para el acceso a ficheros automatizados, utilización de datos cifrados y el control de las actividades ilícitas o inusuales observadas en los ficheros) [246].

La determinación del nivel de seguridad que deba garantizarse en los ficheros automatizados deberá considerar, por una parte, los progresos técnicos en materia de métodos y técnicas de seguridad propios del ámbito informático, y, por otra, la naturaleza de los datos almacenados en el fichero y los riesgos potenciales. Las medidas de seguridad habrán de ser idóneas; es decir, adaptadas a las propias posibilidades de vulnerabilidad y funciones del fichero, y proporcionadas a los riesgos.

No obstante las previsiones de seguridad apuntadas, la aparición de grandes redes de información, incluso a escala planetaria, exige un replanteamiento urgente de las necesarios criterios de seguridad.

Las telecomunicaciones permiten actualmente el interfuncionamiento y la comunicación a escala global, y ello no sólo supondrá importantes cambios técnicos; si no sobre todo, y fundamentalmente, modificará la forma en que los ciudadanos y la sociedad perciben las relaciones organizativas humanas. Pero esa comunicación global acentúa también la necesidad de contar con una protección adecuada para todos los ciudadanos y los datos a ellos referidos.

Ahora bien, conviene tener presente que la evolución técnica es de tal magnitud y rápidez que el Derecho dificilmente puede adaptarse con la misma celeridad y cumplir todas las exigencias que se le reclaman. En esta materia parece cumplirse aquel sempiterno reproche que se hace a la normación jurídica, por ir generalmente a remolque de la realidad de las cosas. Pero el Derecho, por su imprescindible papel en la ordenación de la vida colectiva de los pueblos, no puede estar sometido a vaivenes más o menos oportunistas, a mutaciónes constantes.

[246] Las imperfecciones de los métodos y medidas de seguridad enumerados han propiciado, también como resultado de la rápida evolución técnica, el surgimiento de nuevos métodos, tales como la verificación de la firma, reconocimiento de la voz, reconocimiento de las huellas digitales y otros métodos tales como el reconocimiento de huellas de la palma de la mano, de la retina, etc. Vid. Conseil de l´Europe, *Les nouvelles tecnologies: un défi pour la protection de la vie privée?*, Strasbourg, 1989, p. 40.

Su fuerza radica precisamente en la estabilidad que aporta, al señalar el marco dentro del cual deberán producirse las relaciones entre los hombres; y que como el hombre debe atender a su esencia, y no a sus puntuales manifestaciones.

No obstante esta matización, ello no debe entenderse como un inoperante inmovilismo, como la negación de la necesaria consideración histórica de los procesos sociales. Más bien supone una llamada de atención para que asumamos nuestras propias responsabilidades. En un sector como éste de constantes cambios, al que el Derecho no puede llegar si no con retraso, se revela imprescindible una conciencia social informada, crítica, que sea capaz, olvidando "los cantos de sirenas", de rebelarse contra las modas impuestas, las necesidades creadas artificialmente; en definitiva, contra las vulneraciones de sus derechos y de exigir el efectivo y total cumplimiento de los mismos.

Dos consideraciones, por último, deben tenerse en cuenta a la hora de pretender articular una regulación de estos novedosos procesos tecnológicos:

a. En lo tocante a la existencia y funcionamiento de las grandes redes de telecomunicación el primer problema estriba en determinar a quien corresponde adoptar las medidas de seguridad. Ningún Estado es responsable del funcionamiento global del sistema, sólo le compete establecer los requisitos materiales y formales que deberán cumplir los usuarios de su territorio para conectarse al sistema.
   Ni siquiera en la hora presente se conoce la "longitud" de estas redes, ni el número de sus usuarios. Sin olvidarnos del elevado nivel de "basura" que suele encontrarse en el periplo por estas "autopistas de la información" [247].
b. Respecto a los ciudadanos, a los riesgos inherentes a las posibilidades de tratamiento y comunicación global de sus datos personales recogidos en cualquier punto del planeta, sin posibilidad real de ejercitar los derechos que les asisten o exigir las responsabilidades que se deriven de un mal uso de sus datos, se une la dimensión constituida por la consideración de los ciudadanos como "usuarios" del sistema. Ya no nos limitamos a suministrar datos, si no que somos a la vez usuarios de los mismos. Esa utilización, que exige un control, supone también una fuente adicional de datos personales. La facturación o el cobro de los servicios recibidos a través de estas redes, incorporará datos relativos a la naturaleza del servicio, la dirección del usuario, las "preferencias de consulta", sus relaciones con otros usuarios a través del sistema, etc.

[247] Así con respecto a Internet -¿panacea de la comunicación o gran basurero imformático?- se ha indicado como no se ha hecho famoso precisamente por sus prestaciones de utilidad: programas pornográficos de libre acceso, posibilidades de fabricar un potente explosivo siguiendo sus instrucciones, mensajes de organizaciones y grupos terroristas, la CIA ansiosa por controlar todos los ficheros de correspondencia electrónica. A ello se une un número considerable de "fisgones" y "delincuentes" que generan pérdidas millonarias decodificando los lenguajes criptográficos que protegen el acceso a la red. En definitiva, *un cúmulo de mediocridades y mucho de notoriedad.* Cfr. MEDINA, L., "El laberinto cibernético", en *La Revista,* núm. 1, 22 de octubre de 1995, p. 131-134. La cursiva es nuestra. Asimismo, PEREZ LUÑO, A.E., "Internet: Navegaciones y Abordajes", en ABC Sevilla, lunes 28 de octubre de 1996, p. 82; y NEGROPONTE, N., El mundo digital, Ediciones B, Madrid, 1996.
Para el ámbito comunitario, vid. especialmente las consideraciones acerca de los contenidos "indeseables" en Internet, y que aparecen recogidos en Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Contenidos ilícitos y nocivos en Internet, COM (96) 487 final, Bruselas, 16.10.1996.

En definitiva, en materia de seguridad de la información debe cumplirse aquel viejo adagio a tenor del cual "a nuevos males, nuevos remedios".

5.5. El flujo transfronterizo de datos.

La transmisión de datos personales de un país a otro es un aspecto de la nueva problemática que ha de ponerse de relieve, dada su importancia creciente [248].

Si como se ha manifestado, el volumen de datos personales en circulación ha aumentado considerablemente, también es cierto que la circulación o flujo transfronterizo de tales datos se ha igualmente desarrollado y continuará haciéndolo.

Si bien antes del desarrollo de la informática ya existía un flujo internacional de informaciones constituida por datos personales, la automatización de la recuperación y la transmisión de tales datos revela la dimensión internacional de un problema ya conocido: la protección de los datos personales frente a un proceso de tratamiento automatizado [249].

Para entender este fenómeno conviene tener en cuenta que la circulación internacional de datos personales es un fenómeno de naturaleza compleja: puede afectar a las condiciones de la competencia en el mercado; puede constituir en sí misma una violación de los derechos de los ciudadanos; puede ser necesaria a los fines de un necesario auxilio judicial; puede afectar a la investigación en determinados sectores, etc. [250]. Pero tampoco debe olvidarse que en la práctica la protección de las personas pierde eficacia y disminuyen las posibilidades de control a medida que se amplía el ámbito geográfico de la protección.

A ello hay que añadir el hecho de que nos encontramos ante un conflicto entre dos intereses claramente delimitados: el de la industria de la información (que exige la libre circulación de datos, pues cualquier tipo de control puede incidir en una obstrucción al desarrollo del mercado), y el de las personas cuyos datos pue-

[248] Cfr. FROSINI, V., "Banco de datos y tutela de la persona", cit., p. 37.
[249] Cfr. *Flujo Internacional de Datos. Recomendación de la OCDE,* cit., p. 8.
[250] Cfr. CARRASCOSA GONZALEZ, J., "Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho Internacional Privado", en *Revista Española de Derecho Internacional,* vol. XLVI, núm. 2, 1992, pp. 417-441.

den ser objeto de transmisión (que exigimos una circulación restringida y controlada en aras de la protección de nuestros derechos e intereses legítimos).

Ante esta problemática surgió la necesidad de articular una serie de mecanismos legislativos y técnicos que posibiliten una convivencia entre el necesario flujo de informaciones y el respeto de los derechos de los ciudadanos [251].

Ahora bien, esta solución no podrá ser correctamente articulada si no partimos de un hecho fácilmente constatable: la desigualdad de las relaciones interestatales. Las relaciones entre países productores y países consumidores de tecnologías informáticas constituye uno de los problemas más importantes de la civilización informática, que abarca todo el planeta, aunque de una manera muy desigual entre los distintos países [252]. Así frente a los Estados tecnológicamante desarrollados, productores de información, nos encontramos con aquellos de tecnología atrasada, meros receptores y consumidores de información.

Estas desigualdades, que están produciendo todo un movimiento de neocolonización cultural, no sólo se reducen a lo técnico, sino que se amplían a lo jurídico. La ausencia de una conciencia tecnológica acarrea, de manera consecuente, la ausencia de una conciencia de los riesgos que las nuevas tecnologías pueden suponer para los derechos y libertades de los ciudadanos. De ahí la ausencia de legislaciones protectoras de los datos personales.

Ante esta situación, la normativa protectora de datos de los Estados desarrollados presentan, en esta materia, un carácter especialmente preventivo. Se trata de impedir que datos recogidos o tratados en un Estado salgan de su territorio buscando amparo en otros Estados sin una legislación específica, o con unos inferiores niveles de protección. Pero los actos de vulneración pueden también producirse en terceros Estados destinatarios de los datos. Esta situación se producirá cuando el Estado al que se transfieran legítimamente los datos sea utilizado como *Estado-puente* para la posterior transmisión a terceros países, rompiendo de este modo la posibilidad de aplicación de los mecanismos de control y verificación respecto de la transmisión de datos [253]. No obstante, el planteamiento no es en ocasiones del todo respetado. En numerosas ocasiones, y gracias al desarrollo de las telecomunicaciones, estos *"paraísos informáticos"* son protegidos y utilizados por múltiples operadores para obviar el control que sus legislaciones les impondrían y actuar de acuerdo a sus únicos, exclusivos y excluyentes intereses. De esta forma todos contentos: los Estados cumplen asegurando la protección de los datos personales

[251] Cfr. ESTADELLA YUSTE, O., *La protección de la intimidad frente a la transmisión de datos personales*, cit., y RIPOLL CARULLA, S., *Las libertades de información y de comunicación en Europa*, cit.

[252] Cfr. FROSINI, V., "Banco de datos y tutela de la persona", cit., p. 38.

[253] Cfr. CARRASCOSA GONZALEZ, J., "Protección de la intimidad y tratamiento automatizado de datos...", cit., p. 426.

tratados en su territorio; la existencia de "paraísos informáticos" permite a los operadores obviar su legislación nacional, ante la incompetencia del Estado de origen de los datos de inmiscuirse en la regulación de un fenómeno que tiene su "origen" en otro Estado "soberano". La hipocresía es manifiesta.

Pese a lo señalado, el criterio generalmente utilizado es el de la reciprocidad; es decir, la transferencia de datos personales de un Estado a un tercer país sólo podrá efectuarse cuando éste garantice un nivel de protección adecuado; o bien cuando preste las garantías adecuadas que aseguren la protección de los datos personales. No obstante, como en otros sectores, las garantías dejan en ocasiones paso a otros intereses, económico-políticos, que se imponen sobre la necesaria defensa de los derechos de los ciudadanos.

Queda bien patente la necesidad de una correcta y global regulación del flujo transfronterizo de datos. Cuando los diferentes Estados hayan establecido una protección uniforme y adecuada de los ciudadanos en relación a posibles abusos informáticos, los datos podrán circular libremente. Esa protección uniforme exige también una posición común para el flujo de datos, tanto activo como pasivo, con terceros países .

Tal uniformidad podría venir dada por la elaboración de un Convenio internacional que, partiendo de las experiencias internacionales convencionales previas (v.g. Recomendación OCDE y Convenio 108 del Consejo de Europa), no pretenda resolver exclusivamente los problemas derivados del flujo de datos personales, sino que incluyera además como aspiración última una puesta en común más justa y equitativa de las innovaciones tecnológicas, como uno de los motores del desarrollo social, económico y cultural de los más desfavorecidos.

5.6. *Instrumentos de garantia. La autoridad de control.*

El reconocimiento a los ciudadanos de su derecho a la autodeterminación informativa no basta por sí mismo para asegurar el efectivo respeto y cumplimiento del mismo. La posición de inferioridad en que se halla el ciudadano frente a los grandes operadores informáticos, tanto públicos como privados, supone *de facto* un serio obstáculo para el despliegue de sus derechos.

Ante esta situación, la mayoría de las legislaciones han introducido unos organismos de control, encargados de verificar el correcto funcionamiento de los ficheros y asegurar la efectividad de los derechos que las propias legislaciones protectoras reconocen a los ciudadanos. No obstante, esos mecanismos de control difieren notablemente tanto en su naturaleza como en sus atribuciones.

En algunas legislaciones se confía a los ciudadanos el acudir directamente a los tribunales de justicia para la restitución de sus legítimos derechos e intereses ante abusos informáticos. Otras veces se trata de un organismos administrativo. Pero

la mayoría de las legislaciones prevén un órgano independiente [254], de naturaleza individual o colectiva.

Es la independencia la característica esencial que debe imperar en la creación de una autoridad de control. Esa independencia debe ser completa; es decir, reconocida tanto a nivel orgánico, como funcional y presupuestario.

Pero esa "independencia" se ve a menudo defraudada cuando se constata la modalidad de elección de tal organismo. La dependencia gubernamental supone un grave atentado a esa autonomía y coarta las posibilidades de actuación de tales órganos en defensa de los derechos de los ciudadanos.

Así con respecto a la Agencia de Protección de Datos española, ha señalado Pérez Luño como su regulación supone uno de los aspectos más negativos de la protección de datos en nuestro país. Pese a que la Exposición de Motivos señala la "absoluta independencia" de su Director, sin embargo éste no es nombrado por el Parlamento, sino por el gobierno, a quien corresponde asimismo su cese. Además sus informes anuales no los presenta tampoco ante el Parlamento, sino que lo deberá hacer ante el Ministerio de Justicia. Todo ello condiciona, continúa señalando Pérez Luño, la propia neutralidad y credibilidad de esa institución, que aparece como un mero delegado gubernativo para la informática [255].

Respecto a sus misiones primordiales destacan la de velar por el cumplimiento de la ley, sancionar las infracciones de carácter administrativo previstas en ella y atender las reclamaciones de los interesados. Para ello deberá dotarse a estas autoridades de los medios de investigación e intervención con respecto a los responsables de los tratamientos y bajo el control de las autoridades judiciales [256].

La facultad de investigación debe permitir a la autoridad de control recabar de los responsables del tratamiento los datos necesarios para el cumplimiento de su cometido. Esta facultad se manifiesta concretamente en el acceso a los datos que son objeto de tratamiento.

Para conseguir un adecuado respeto de los derechos de la persona resulta evidente la necesidad de que la autoridad de control disponga de un poder de intervención efectivo: poder de ordenar el bloqueo o la supresión de datos, de prohibir un tratamiento, etc.

[254] Cfr. PEREZ LUÑO, A.E., "Informática jurídica y derecho de la informática en España", cit., p. 94; *ID.*, "La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo", cit., pp. 286-289.

[255] Cfr. PEREZ LUÑO, A.E., "Comentario Legislativo: La LORTAD y los derechos fundamentales", cit., pp. 413-414. Asimismo, CASCAJO CASTRO, "Tratamiento automatizado de los datos de carácter personal", cit., pp. 372-374; y TASENDE CALVO, J.J., "Notas al Proyecto de Ley Orgánica de regulación...", cit., p. 111.

Además, debe dotarse a la autoridad de control del poder de recurrir a la autoridad judicial cuando constate la existencia de infracciones a las disposiciones de las leyes protectoras de los datos personales. Derivado de su facultad de investigación, resultaría extraño que una autoridad encargada de proteger los derechos de la persona no pudiera recurrir a la autoridad judicial cuando tenga constancia de una infracción contra tales derechos; amén del derecho de cualquier persona de presentar una denuncia ante la autoridad de control, y que esta denuncia pueda llegar ante la autoridad judicial.

Tras la reciente y progresiva inclusión en los nuevos Códigos Penales de los denominados "delitos informáticos", debería reconocerse a las autoridades de control la legitimación activa para iniciar un procedimiento contra aquellas actividades delictivas que tengan por objeto la violación de los derechos de los ciudadanos cometidas por medios informáticos. Asimismo en los procedimientos iniciados por los particulares debería reconocérsele la facultad de actuar como coadyuvantes, en defensa de la "legalidad informática" y los derechos de los ciudadanos.

Por último, es de una notable importancia que la autoridad de control pueda presentar de manera periódica, con un intervalo máximo de un año, de un informe sobre sus actividades, donde se pongan de manifiesto los problemas planteados por la aplicación de las leyes de protección de datos, las actividades de la autoridad de control, el nivel de reclamaciones formuladas por los particulares, así como las líneas directrices que deberán seguirse en el futuro.

5.7. *Las limitaciones del derecho a la libertad informática: exigencias ineludibles de las medidas restrictivas.*

Todas las leyes de protección de datos contienen algún tipo de excepciones a la aplicación de sus normas [257], tipificando las situaciones en las que por razones de seguridad, para la defensa de la democracia y el orden constitucional o para la defensa de los derechos de los demás se podrá limitar o suspender el derecho a la libertad informática [258].

En el ámbito convencional internacional el Convenio 108 del Consejo de Europa establece a este respecto, que podrán, dejarse sin efecto sus preceptos relativos a

[256] Cfr. HEREDERO HIGUERAS, M., "La Agencia de Protección de Datos", en *Informática y Derecho,* núms. 6-7, 1994, pp. 323-357. Asimismo, CASTILLO JIMENEZ, C., "Estatuto de la Agencia de Protección de Datos (Real Decreto 428/1993)", ibíd., pp. 359-364.

[257] Cfr. PEREZ LUÑO, A.E., "Informática jurídica y derecho de la informática en España", cit., p. 97.

[258] Para un estudio histórico de las limitaciones de los derechos fundamentales en función de la defensa de los intereses del Estado, vid. CRUZ VILLALON, P., *El estado de sitio y la Constitución (La constitucionalización de la protección extraordinaria del Estado (1789-1878),* Centro de Estudios Constitucionales, Madrid, 1980.

calidad de los datos, datos sensibles y derechos de los afectados cuando así estuviere previsto en la legislación de las Partes contratantes, y constituyera una medida necesaria en una sociedad democrática para la protección de la seguridad del Estado, la seguridad pública, los intereses monetarios o la represión de los delitos, así como para la protección del interesado y de los derechos y libertades de otros (art. 8.2).

Se consagra de este modo la posición a tenor de la cual no existe un derecho absoluto ni una soberanía irrestringible sobre los propios datos, ya que la personalidad del individuo se desenvuelve dentro de la sociedad y de la comunidad, y ha de aceptar ciertas limitaciones. Ahora bien, esta naturaleza "limitada" no debe suponer en ningún caso una quiebra de la libertad informática.

La apelación a la defensa de determinados valores o intereses colectivos, no debe ser óbice para un uso torticero de las habilitaciones legales. La propia indefinición de los supuestos en los que es tolerable esa "limitación", coadyuva a la necesidad de una aplicación estricta de los mismos.

Así, como ha señalado Rigaux, del interés general debe distinguirse claramente el interés del Estado. Mientras que el primero señala los valores comunes a la colectividad política y a la sociedad civil, valores inscritos en los textos constitucionales e internacionales, el interés del Estado señala la permanencia de las instituciones políticas y su protección frente al enemigo exterior. No obstante, cuando los detentadores del poder invocan el interés del Estado, la seguridad pública o la seguridad nacional para legitimar la limitación de determinados derechos fundamentales, están particularmente expuestos a confundir este interés con la perpetuación del poder del que están democráticamente investidos [259].

En este sentido, si bien dichas limitaciones han de ser aceptadas, las mismas están sujetas a determinados requisitos que, ya desde lo señalado por el Convenio de 1981 del Consejo de Europa y el *Bundesversfassungeritchs* en su referida Sentencia sobre la Ley del Censo de Población de 1983, pueden sistematizarse en dos ineludibles y concretas exigencias:

a. Un fundamento legal, del que pueda deducirse con claridad y de forma inteligible para el ciudadano los supuestos y el ámbito de las limitaciones, y que responda, por tanto, al imperativo de claridad normativa inherente al Estado de Derecho [260].

[259] Cfr. RIGAUX, F., "Introduction Generale", en *Revue Trimestrielle des droits de l´homme*, núm. 13 (monográfico "La liberté d´expréssion, son étendue et ses limites), janvier 1993, p. 17.

[260] Cfr. TORNE-DOMBIDAU JIMENEZ, J., y CASTILLO BLANCO, F.A., "Informática y protección de la privacidad del individuo (II)", en *Actualidad Administrativa*, núm. 22, 7-13 de julio 1993, p. 281; PEREZ LUÑO, A.E., *La Seguridad Jurídica*, 2ª edic. revisada y puesta al día, Ariel, Barcelona, 1994.

A este respecto, el TEDH ha realizado unas importantes precisiones señalando como la expresión "prevista por la ley" indicada en el párrafo 2 del art. 8 del CEDH, implica que no basta con que la injerencia en los derechos esté prevista por una norma nacional, si no que ésta debe ser accesible al interesado, quien debe, además, poder prever las consecuencias que pueda tener para él. Además, cuando su práctica se realiza por medio de medidas secretas, que escapan al control de las personas afectadas, la misma ley debe definir el ámbito del poder atribuido a la autoridad competente con bastante claridad para proporcionar al individuo una protección adecuada contra la arbitrariedad [261].

b. Ha de utilizarse el principio de proporcionalidad en la restricción de estos derechos fundamentales; es decir, que la medida sea adecuada - necesaria en una sociedad democrática - y, además, indispensable para la consecución de los respectivos y predeterminados fines. La interferencia que lleve aparejada no puede ser desproporcionada a la importancia del objeto y a las cargas que imponga al ciudadano.

El concepto de necesidad implica, según reiterada jurisprudencia del TEDH, una exigencia social imperiosa; y sobre todo, la medida tomada debe ser proporcionada a la finalidad legítima perseguida. Además, el alcance del margen discrecional que tienen las autoridades no depende solamente de la finalidad de la restricción, si no también de la naturaleza del derecho de que se trate [262].

Por su parte, la regla de la proporcionalidad es de observancia obligada para proceder a la limitación de un derecho fundamental. Ello conduce a la negación de la legitimidad de aquellas limitaciones que incidan en el ejercicio de los derechos fundamentales de forma poco comprensible, de acuerdo con una ponderación razonada de bienes y proporcionada de los mismos en relación con el contenido y finalidad de la medida restrictiva [263].

Por otra parte, las limitaciones del derecho no deben ser de tal calado que supongan un menoscabo de su contenido esencial. De nada sirve el reconocimiento de los derechos a favor de los ciudadanos si se limita su ejercicio de forma que, más que una limitación, debamos hablar de una derogación encubierta, de su propia naturaleza, atributos y funciones.

[261] Sentencias, *Silver y otros*, de 25 de marzo de 1983; Malone, de 2 de agosto de 1984; y *Leander*, de 26 de marzo de 1987.

[262] Sentencias, *Lingens*, de 8 de julio de 1986; *Gillow*, de 24 de noviembre de 1986; y *Leander*, de 26 de marzo de 1987.

[263] Cfr. GOMEZ TORRES, C., "El abuso de los derechos fundamentales", en la obra colectiva, edic. a cargo de A.E. Pérez Luño, *Los derechos humanos: significación, estatuto jurídico y sistema*, Publicaciones de la Universidad de Sevilla, Sevilla, 1979, pp. 301-332. Asimismo, TORNE-DOMBIDAU JIMENEZ y CASTILLO BLANCO, F.A., "Informática y protección de la privacidad...", cit., p. 283.

Tal y como ha señalado Pérez Luño, y siguiendo la doctrina de nuestro Tribunal Constitucional, "dos acepciones pueden distinguirse de la noción de "contenido esencial": la primera equivalente a "naturaleza jurídica de cada derecho", que se considera preexistente al momento legislativo; la segunda a "intereses jurídicamente protegidos", en el sentido de que se lesionaría 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" [264].

Ante la proliferación y constante apelación por parte de las autoridades públicas a estas limitaciones conviene insistir, siguiendo nuevamente a Pérez Luño, en el carácter excepcional de estos supuestos; en que su razón de ser no puede ser otra que la conservación del orden democrático; y en que la existencia de tal motivación no puede quedar en manos de la Administración, sino que debe quede ser reconocida por los Parlamentos como depositarios de la soberanía popular [265].

Como conclusión, debe tenerse presente que estas limitaciones suponen *de facto* otorgar a los poderes públicos la posibilidad de actuar, generalmente de forma secreta, al margen de los mecanismos de control establecidos en las sociedades democráticas. Ello ha llevado al TEDH ha afirmar la necesidad de establecer unas garantías adecuadas y suficientes contra los abusos, ya que un sistema de control destinado a proteger la seguridad nacional crea el riesgo de socavar, e incluso destruir, la democracia con el argumento de defenderla [266].

[264] Cfr. PEREZ LUÑO, A.E., *Los derechos fundamentales*, 3ª edic., Tecnos, Madrid, 1988, p. 77.
[265] Cfr. PEREZ LUÑO, A.E., "Informática jurídica y derecho de la informática en España", cit., p. 97.
[266] Vid. entre otras las Sentencias, *Klass y otros*, de 6 de septiembre de 1978; y *Leander*, de 26 de marzo de 1987.

SEGUNDA PARTE

EL DERECHO A LA LIBERTAD INFORMÁTICA EN LA UNIÓN EUROPEA

A. LA PROTECCION DE LOS DATOS PERSONALES EN LA UNION EUROPEA.

1. INTRODUCCION. EL LARGO DEBATE INSTITUCIONAL.

El uso más frecuente e intensivo del tratamiento de datos personales, unido a la necesidad de intercambio de datos hacen indispensable la aplicación en la Unión Europea de medidas tendentes a garantizar la protección de los derechos de los ciudadanos en lo referente al tratamiento automatizado de sus datos personales.

La articulación de esas medidas no ha sido, sin embargo, una cuestión sencilla. En un proceso que se ha desarrollado durante más de dos lustros, han sido constantes los avances y retrocesos, los cambios de opinión, los estancamiento y las prisas.

Sería por ello interesante que nos detengamos en los principales hitos que han jalonado este proceso, y que no son más que el reflejo de la distinta concepción que respecto al estatuto de los derechos fundamentales, y por ende al derecho a la libertad informática, han tenido las distintas instituciones comunitarias desde el origen mismo de la Comunidad.

Desde 1973, las diversas instituciones comunitarias promulgaron disposiciones diversas [1] acerca de las implicaciones que la informática podía tener para la

[1] De entre las más relevates en este iter legislativo vid., Commission des Communaútes européennes. Une politique communautaire de l´informatique, SEC (73) 4300 final; Resolución del Parlamento Europeo de 21 de febrero de 1975, JOCE, nº C 60, 13 mars 1975, p. 48; Resolución del Parlamento Europeo de 8 de mayo de 1979, JOCE, nº C 140, 5 juin 1979, pp. 34-38.

Aprobado el Convenio del Consejo de Europa sobre la protección de las personas respecto al tratamiento automatizado de los datos de carácter personal, la Comisión Europea en su Recomendación, de 29 de Julio de 1981, subrayaba el carácter de derecho fundamental de dicha protección y recomendaba a todos los Estados miembros que ratificasen el precitado Convenio. Cfr. DOCE nº L 246/31, 29.8.81., p. 77. Asimismo, la Resolución de 9 de marzo de 1982, JOCE, nº C 87/39, 5.4.82. Especialmente interesante resulta la propuesta que lanzaba

Comunidad y para sus ciudadanos. Durante casi dos lustros asistimos a una situación de cierta indefinición sobre estas cuestiones. No obstante, todas estas posiciones desembocaron en 1990 en la elaboración por parte de la Comisión, junto a otras medidas de acompañamiento, de la Propuesta de Directiva del Consejo de 27 de julio de 1990 relativa a la protección de las personas en lo referente al tratamiento de datos personales [2].

Los objetivos perseguidos por esas propuestas eran fundamentalmente : a) aproximar y armonizar las disposiciones interiores legislativas y reglamentarias sobre protección de la intimidad de las personas frente a la informática a través de una "Directiva general"; b) promover a través de una "Directiva sectorial" una normativa sobre redes públicas digitales de telecomunicaciones; c) lograr la seguridad de los sistemas de información, y d) promover la adhesión de la CEE al Convenio 108 del Consejo de Europa [3].

Los dictámenes del Comité Económico y Social [4] y del Parlamento [5] introdujeron numerosas modificaciones en el texto de la Propuesta de Directiva de 1990. El Parlamento en su dictamen pedía, especialmente, que el tratamiento de los datos personales pudiera efectuarse a condición, entre otras cosas, de que la persona afectada hubiese dado explícita o implícitamente su consentimiento, también en cuanto al contenido sustancial de los datos a ella referido. Además, insistía de modo particular en el principio de que los sistemas de tratamiento automatizado debían estar al servicio del hombre y respetar, por consiguiente, los derechos y libertades individuales, la identidad de la persona y la vida privada [6].

---

en su punto 12, cuando, en su redacción original en lengua francesa, señalaba: "estime que l´on peut utilement envisager d´examiner si le droit à la protection des données personnelles ne peut et ne devrait pas expressément figurer, en tant que droit de l´homme et droit fondamental dans la liste de la convention européenne des droits de l´homme et des libertés fondamentales sous forme de sixième protocole additionnel".

Resoluciones del Parlamento Europeo de 26 de marzo de 1984, DOCE, nº C 117/84, 30.3.84.

Por su parte el Consejo Europeo de Estrasburgo, de los días 8 y 9 de Diciembre de 1989 destacó, al discutir ciertas medidas en favor de la libre circulación de las personas y de la Europa de los ciudadanos, la necesidad de velar porque la colaboración entre las Administraciones garantice previamente la protección de los ciudadanos por lo que se refiere a la utilización de los datos personales.

[2] Cfr. COM (90) 314 final - SYN 288, Bruselas, 24 de septiembre de 1990. Como medidas de acompañamiento a la Propuesta de Directiva destacaban la "Propuesta la Directiva del Consejo relativa a la protección de los datos personales y de la intimidad en relación con las redes digitales públicas de telecomunicación y, en particular, la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas"; la "Propuesta de Decisión del Consejo en el ámbito de la seguridad de la información"; y la "Recomendación de Decisión del Consejo relativa a la apertura de negociaciones con vistas a la adhesión de las Comunidades Europeas al Convenio del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de los datos personales".

[3] Cfr. CARRASCOSA GONZALEZ, J., "Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho Internacional Privado", en Revista Española de Derecho Internacional, vol. XLIV, núm. 2, 1992, p. 435.

[4] Cfr. DOCE nº C 159/38, 17.6.91

[5] Cfr. DOCE nº C 94/173, 13.4.92

[6] Cfr. Fichas Técnicas sobre el Parlamento Europeo..., cit., p. 90.

Las reseñadas modificaciones determinaron a la Comisión a presentar una "Propuesta modificada de Directiva 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" [7]. La Propuesta modificada contiene, entre otras, dos importantes enmiendas solicitadas por el Parlamento Europeo, y que se refieren a:

- el abandono de la distinción formal entre las normas aplicables al sector público y al privado,
- la elaboración de disposiciones relativas a los procedimientos selectivos de notificación a la autoridad de control y a los códigos de conducta.

Estas modificaciones tienen el mérito de indicar claramente que la protección debe ser la misma en todos los sectores afectados.

Tras la entrada en vigor del Tratado de la Unión Europea, las cuestiones relativas al Mercado Interior (art. 100 A), entre las cuales se incluía la Propuesta modificada de 1992, quedaron sometidos al nuevo procedimiento de codecisión (art. 189 B) [8], en virtud del cual el Parlamento y el Consejo debían adoptar de común acuerdo los actos legislativos afectantes a estos ámbitos.

Cumplidas las distintas fases del referido procedimiento, el *iter* legislativo se ha cerrado recientemente con la aprobación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, (en adelante, Directiva del 95) 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 [9].

2. DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 24 DE OCTUBRE, 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.

Corolario de un largo y dubitativo proceso comunitario, la Directiva 95/46 viene a colmar el vacío existente en la legislación comunitaria respecto de la protección de los datos personales [10].

El recurso a una Directiva, como señala Carrascosa González, y al consiguiente "derecho unificado" parece adecuado, ya que, como venimos señalando, existen

[7] Cfr. COM (92) 422 final - SYN 287, Bruselas, 15 de octubre de 1992.

[8] Para una sencilla y expresiva exposición acerca de las diferentes fases de este novedoso proceso legislativo, vid. Comisión Europea, CONFERENCIA INTERGUBERNAMENTAL 1996 - Informe de la Comisión para el Grupo de reflexión, Oficina de Publicaciones Oficiales de las Comunidades Europeas, Luxemburgo, 1995, p. 78.

[9] Cfr. DOCE nº L 281/31, 23.11.95. Se cumplen así, con esta aprobación, las previsiones señaladas por la propia Comisión Europea en su Programa de actuación para 1995. Sobre ello, vid. COM (95) 26 final, 08.02.95.

[10] DOCE Nº L 181/31, 23.11.1995.

Estados con regulación específica en la materia y otros que carecen de ella [11]. No obstante, la aprobación de la Directiva debe suponer un estímulo, y ahora una obligación ineludible, para que aquellos Estados que aún no la poseen elaboren normas internas protectoras de los datos personales, atemperándose a las previsiones legislativas comunitarias [12] [13]. Un "mercado interior" de datos de carácter personal sólo es posible si las legislaciones nacionales se unifican gracias al establecimiento de una Directiva común [14] [15].

Como ha señalado la propia Comisión, esta Directiva se inscribe en el contexto de la creación de un espacio europeo de información en el que el tratamiento de datos personales aumentará de forma sustancial. Así la aparición de las "autopistas de la información" [16] y de "medios de comunicación de masas" creará posibilidades de tratamiento de datos cada vez más intrusivos para la vida privada [17].

Tomando como base las consideraciones que sobre su articulado formuló la propia Comisión Europea a la redacción del año 92, y que ha sido asumido en casi su totalidad por el texto ahora vigente, así como las importantes Enmiendas formuladas en su momento por el Parlamento Europeo [18], nos proponemos acometer

[11] Cfr. LAZPITA GURTUBAY, M., "Análisis comparado de las legislaciones sobre protección de datos de los Estados miembros de la Comunidad Europea", en Informática y Derecho, núms. 6-7, 1994, pp. 397-420.

[12] Cfr. ROSENBAUM, J.I., "The European Commission´s Dreft Directive on Data Protection", en Jurimetrics, Vol. 33, núm. 1, p. 5. Deseo mostrar mi agradecimiento a Dña. Antonia Monge Fernández por su inestimable ayuda en la traducción de esta obra. Asimismo, SIMITIS, S., "From the Market to The Polis: The EU Directive on the Protection of Personal Data", en Iowa Law Review, Vol.80/No.3, March 1995, pp. 47-ss.

[13] La transposición de la Directiva europea de protección de datos al Derecho español y su influencia en el marco normativo diseñado por nuestra LORTAD constituyó el objeto de las Jornadas sobre el Derecho Español de la Protección de Datos Personales(Madrid, 28,29 y 30 de octubre de 1996). Vid. a este respecto, y entre otras, las aportaciones de Pérez Luño, Lucas Murillo de la Cueva y Martín Casallo, en Jornadas sobre el Derecho Español de la Protección de Datos Personales, Agencia de Protección de Datos, Madrid, 1996. Vid., asimismo, SANCHEZ BRAVO, A., "La regulación de los derechos de la persona interesada en la Directiva europea de protección de datos", ibídem, pp. 295-307.

[14] Cfr. CARRASCOSA GONZALEZ, J., "Protección de la intimidad y tratamiento automatizado...", cit., pp. 435-436.

[15] Las divergentes legislaciones nacionales son, además, susceptibles de constituir un obstáculo al flujo transfronterizo de datos, al plantear problemas de conflictos de leyes. Vid. en este sentido, RIGAUX, F., "La loi applicable à la protection des individus à l´egard du traitement automatisé des données à caractère personnel", en Revue Critique de Droit Internationale Privé, 1980, pp. 443-478.

[16] En este sentido, la Comisión Europea ha elaborado un estudio acerca de las repercusiones que en el ámbito de la Unión Europea tendría lo que ya se anuncia como "ciberespacio", y cuya efectiva articulación requerirá un unificación jurídica y técnica. Cfr. COLOM, V., y VAN BOLHIUS, H.E., Cyberspace Reflections, European Commission, DG XIII, Bruselas, 1995.

[17] Comisión Europea. 4551/95 (Presse 32 - G), 6.11.1995, pp. 12-13.

[18] Enmiendas que, formuladas a la Propuesta de 1990, fueron asumidas en parte por la Comisión en su Propuesta modificada de 1992, de donde han pasado otorgando, en numerosas ocasiones, una mayor perfección formal y de contenido a la Directiva que ahora consideramos.

la exposición y comentario de las previsiones que incorpora el articulado de esta, al menos en la cuestión que nos incumbe, importante Directiva.

2.1. *Objetivos y ámbito de aplicación subjetiva.*

La Directiva tiene por objeto establecer una protección equivalente de alto nivel en todos los Estado miembros de la Comunidad a fin de eliminar los obstáculos a los intercambios de datos necesarios para el funcionamiento del mercado interior [19]. Dado que todas las personas gozarán en cada uno de los Estados miembros de una protección equivalente en lo referente al tratamiento de datos personales, los Estados miembros no podrán imponer restricciones a la circulación de dichos datos dentro de la Comunidad invocando la protección del individuo [20].

Tal y como se desprende de su *art. 1*, este objetivo puede desglosarse en los siguientes criterios:

- Los Estados miembros tienen la obligación de garantizar la protección de los derechos y libertades de las personas físicas, y en particular de su derecho a la intimidad, en lo referente al tratamiento de datos personales.
- La protección se garantizará de acuerdo con los mismos principios en todos los Estados miembros y será, por lo tanto, equivalente en todo el territorio comunitario.
- La Directiva intenta conciliar los imperativos de la realización del mercado interior con los de la protección de las personas.

Esta "liberalización" en el intercambio de datos personales, nos sitúa *prima facie* más que ante una norma protectora de los derechos de los ciudadanos, ante lo que parece ser una norma habilitante para que los operadores, fundamentalmente económicos, desarrollen sus actividades. La invocación de la tan traída consecución del mercado interior, sirve en la Comunidad para que cuestiones de importancia capital, sean tratadas, e incluso encuentren su base jurídica, en aquellos

Las alegaciones y Enmiendas del Parlamento pueden encontrarse en su Dictamen sobre la propuesta de la Comisión al Consejo referente a una directiva relativa a la protección de las personas en lo referente al tratamiento de datos personales. Cfr. DOCE Nº C 94/198, 13.4.1992.

Nuestras referencias a las Enmiendas del Parlamento Europeo deben entenderse hechas con referencia al contenido y siguiendo la numeración de las contenidas en el referido Dictamen.

[19] Definido éste en el artículo 7 A del TCE como "espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estará garantizada de acuerdo con las disposiciones del presente Tratado".

[20] En la Propuesta modificada de 1992 se introdujo la expresión, asumida casi en la integridad de su articulado por la Directiva del 95, "y a la libre circulación de los datos", para puntualizar y recalcar que el objetivo de la entonces Propuesta era la instauración y el funcionamiento del mercado interior, mediante una armonización que garantice la protección de las personas.

preceptos del Tratado referidos a cuestiones económicas y monetarias. Se obvia de esta manera una correcta consideración de las consecuencias jurídicas y sociales que para los derechos fundamentales de los ciudadanos puedan derivarse de estos procesos.

Respecto a lo que podríamos denominar como *ámbito subjetivo*, la protección que pretende articular la Directiva sólo recae sobre las personas físicas. Así lo ratifica su *Considerando 24* al señalar "que las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que la conciernan no son objeto de la presente Directiva".

El Derecho comparado no ofrece una solución unitaria a esta cuestión, ya que si en unos países se excluye a las personas jurídicas entre los titulares del derecho a la libertad informática, en otros se ha optado por su inclusión[21].

No obstante puede considerarse a las personas jurídicas como sujetos de derechos, entre los cuales cabría incluir su "derecho a la libertad informática". Como ha señalado Lucas Murillo de la Cueva, las personas jurídicas no son sino instrumentos de los que se valen los hombres para alcanzar determinados fines que de otro modo sería difícil conseguir. Uno de ellos podría se el logro de una defensa conjunta y de una sola vez de determinado aspectos de la autodeterminación informativa[22]. Además, la vulneración de sus "datos personales", si bien no puede menoscabar su intimidad, al menos en la consideración tradicional de ésta, si puede afectar a otros intereses dignos de protección, tales como intereses económicos o morales. Además, como hemos visto anteriormente la protección de la Directiva se extiende no sólo al derecho a la intimidad, si no a los derechos y libertades de los interesados, acogiendo una concepción ciertamente amplia y extensiva.

2.2. *Definiciones.*

Recogidas en su *art. 2* acoge los principales conceptos utilizados en la Directiva. Las definiciones parten de las del Convenio 108 del Consejo de Europa, así como de las recogidas en la mayor parte de las legislaciones de los Estados miembros, añadiendo sin embargo las adaptaciones y precisiones necesarias para garantizar una protección equivalente y de alto nivel en la Comunidad.

[21] Entre los países que excluyen a las personas jurídicas, indicar Alemania, España, Francia, Irlanda, Países Bajos, Portugal, Reino Unido y Suecia. Entre los que las incluyen, Austria, Dinamarca, Islandia, Luxemburgo, Noruega. Tomo la referencia de LUCAS MURILLO DE LA CUEVA, P., Informática y protección de datos personales, Centro de Estudios Constitucionales, Madrid, 1993, p. 50.

[22] Ibidem, p. 51. Asimismo, MIRABELLI, G., "In tema di tutela dei dati personali (Note a margine della Proposta modificata di Direttiva CEE), en Il Diritto dell´informazione e dell´informatica, anno IX, Nº 3, maggio-giugno 1993, pp. 610-613.

El tratamiento de datos personales "sensibles" podrá, en aplicación de tales excepciones, efectuarse en los siguientes supuestos:

a. El interesado ha consentido de manera explícita en dicho tratamiento. Dicho consentimiento deberá ser especialmente informado, para dar a conocer al interesado y hacerle comprender los riesgos que para sus derechos e intereses puedan derivarse de un tratamiento de tan especial categoría de datos. También se permitirá, como una manifestación concluyente de ese consentimiento, un tratamiento de datos sensibles cuando se refiera a datos que el interesado haya hecho manifiestamente públicos.

b. Cuando sea necesario un tratamiento de datos sensibles para el cumplimiento de determinadas obligaciones y derechos del responsable del tratamiento en materia laboral. Como requisito suplementario se exige que tal posibilidad este autorizada por una ley, que, además, deberá establecer garantías adecuadas.
Esta habilitación responde a lo que el Consejo denomina "necesidades" justificadas [46].
Pese a todas estas "garantías", resulta sorprendente cual sea la utilidad de determinados datos sensibles en el ámbito laboral, si no es para producir situaciones de discriminación. Así la pertenencia a organizaciones sindicales, puede llevar a la calificación de un sujeto como "conflictivo"; determinadas dolencias, no incompatibles con el correcto desempeño de una determinada actividad, pueden "desaconsejar" la contratación de un trabajador, etc.

c. El tratamiento es necesario para salvaguardar el interés vital del interesado o de otra persona, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.
Este impreciso precepto debería haberse perfilado con el señalamiento para el que efectúe un tratamiento de tales datos de la obligación de comunicar a la Autoridad de control tal proceso, para que ésta pudiera verificar la pertinencia o no de tal tratamiento, y sobre todo, de la concurrencia de la necesidad de salvaguardar ese interés vital.

d. El tratamiento de datos sensibles lo pueden efectuar fundaciones o asociaciones o cualquier otro organismo de carácter político, filosófico, religioso o sindical, para la consecución de sus objetivos legítimos, pero siempre que se refiera exclusivamente a los miembros y corresponsales de la fundación o asociación que hayan consentido en participar y que los datos no se comuniquen a terceros [47].

[46] Cfr. Posición Común (CE) Nº 1/95, adoptada por el Consejo el 20 de febrero de 1995..., cit., p. 22.

[47] Recoge la Enmienda número 149 del Parlamento Europeo.

e. El tratamiento sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

Respecto a los datos "médicos", se establece una excepción a la prohibición del tratamiento de datos referentes a la salud o a la vida sexual con el fin, como señaló el propio Consejo, de responder a necesidades justificadas en el ámbito médico, sin perjuicio de las garantías adecuadas [48].

El tratamiento de estos datos, asumiendo una concepción ciertamente amplia, estará por lo tanto tolerado cuando resulte necesario para la prevención o diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios. Respecto a la inclusión de los datos de gestión en tal habilitación de tratamiento, nos parece desorbitada, por cuanto irán referidos al desempeño de funciones fundamentalmente administrativas, a cuyo desenvolvimiento poco coadyuvará el conocimiento de determinados datos "sensibles", a no ser que se utilicen como mecanismos de control de determinados sectores de población.

Quizás para compensar ese excesiva amplitud, el precepto establece como mecanismo corrector, y a la vez protector, de los intereses y derechos de los ciudadanos, que dicho tratamiento sea realizado, bien por un profesional sanitario sujeto al secreto profesional, bien por otra persona sujeta asimismo a una obligación equivalente de secreto.

Si el nivel de excepciones establecido para el tratamiento de datos "sensibles" parecía quedar completado, con los supuestos anteriormente señalados, observamos estupefactos como en el apartado 4 se recogen unas denominadas *"excepciones por motivos importantes de interés público"*. En virtud de las mismas, los Estados miembros podrán establecer cuantas limitaciones crean conveniente a la prohibición general de tratamiento de datos "sensibles". Aunque se intenta maquillar apelando al establecimiento de garantías adecuadas (como la notificación de la adopción de la excepciones a la Comisión), esta posibilidad no supone más que una intolerable consagración de la arbitrariedad estatal, para modular, por no decir coartar, los derechos y libertades de los ciudadanos.

El apartado 5 recoge los datos relativos a infracciones, condenas penales o medidas de seguridad [49]. Los tratamientos afectantes a estas categorías de datos sólo podrán realizarse bajo el control de la autoridad pública. Además, dado el carácter particularmente delicado de estos datos, se ha considerado que las excepciones sólo podrían otorgarse mediante disposiciones legislativas en las que se

[48] Cfr. Posición Común (CE) Nº 1/95, adoptada por el Consejo el 20 de febrero de 1995..., cit., p. 22.

[49] Recoge, en parte, la Enmienda número 65 del Parlamento Europeo.

establezcan las garantías apropiadas. Dichas excepciones serán notificadas a la Comisión.

No obstante, para evitar un uso torticero de los datos referidos a condenas penales, se ha introducido un acertado criterio delimitador al establecer que el *registro completo* de tales condenas sólo podrá llevarse bajo el control de los poderes públicos. Se trata con ello de evitar la proliferación de determinadas agencias o instituciones, que al igual que sucede con las agencias que recopilan y "venden" datos sobre insolvencia patrimonial, que se dediquen a la recopilación y suministro de tales datos, con el consiguiente y "estigmatizante" perjuicio para la dignidad y derechos fundamentales de las personas afectadas. Los Estados miembros, podrán ampliar esta previsión a los tratamientos de datos relativos a sanciones administrativas o procesos civiles

Por último, se recoge la propuesta [50] en la que solicitaba a los Estados Miembros que determinen las condiciones en las que podrá utilizarse un número nacional de identificación, en caso de que exista, u otro identificador de carácter general.

2.7. *Confidencialidad y Seguridad del tratamiento.*

A diferencia de la regulación anterior, las disposiciones sobre confidencialidad se han incluido en un artículo aparte (*art. 16*), las relativas a la seguridad, que incumben tanto al responsable como al encargado, se recogen en el *art. 17*.

Respecto al criterio de la confidencialidad, que no se establece expresamente en la redacción, queda reducido al señalamiento de que las personas que actúan bajo la autoridad del responsable o del encargado del tratamiento sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o cuando así se derive de un imperativo legal.

Pero esta regulación, que ya deriva de lo establecido *supra* cuando nos detuvimos en las principales definiciones que incorporaba la Directiva y articulaban sus previsiones, no establece una acertada orientación de lo que deba entenderse, y corresponde a su propia esencia, por confidencialidad.

Más correcto y acertado habría sido indicar la obligación de mantener el secreto profesional a los empleados ("personas que actúan bajo su autoridad") del responsable del tratamiento y otras personas que por razón de su actividad profesional tengan acceso a los datos personales. Estas personas no podrán tampoco comunicar a terceros los datos a los que tengan acceso sin autorización previa del responsable del tratamiento.

[50] Recoge la Enmienda número 65, segunda parte, del Parlamento Europeo.

Respecto a la seguridad de los tratamientos señalar, al igual que se hizo anteriormente, como los peligros que amenazan a los derechos de los interesados no provienen tan sólo del responsable del tratamiento de datos que los recoge, almacena, trata y comunica en su propio interés. También pueden verse amenazados si los datos los utiliza con fines diferentes un tercero que no esté autorizado a acceder a ellos ni a utilizarlos.

El *art. 17* determina a los Estados miembros a establecer la obligación de que el responsable del tratamiento tome las medidas técnicas y organizativas apropiadas y necesarias para la protección contra la destrucción, accidental o ilícita, contra la perdida accidental y contra la alteración, la difusión y el acceso no autorizado, así como contra cualquier otro tratamiento no autorizado de datos personales [51].

Especial interés deberá prestarse a la seguridad cuando el tratamiento incluya la transmisión de datos dentro de una red. Como señaló la Comisión en su Propuesta del año 90, en caso de efectuarse transmisiones de ordenador a ordenador o de ordenador a terminal a través de una red de telecomunicaciones, también deben adoptarse medidas de seguridad con relación a dicha red a fin de garantizar la transferencia segura e ininterrumpida de los datos [52].

Las medidas de seguridad adoptadas deberán garantizar un nivel de seguridad apropiado, teniendo en cuenta, por una parte, los progresos técnicos en materia de seguridad de datos y el coste de la aplicación de esas medidas y, por otra, la naturaleza de los datos y la evaluación de los riesgos potenciales.

La introducción de la consideración de los costes con respecto a las medidas que se vayan a adoptar, supone, a nuestro criterio, un elemento distorsionador para el establecimiento de unas efectivas garantías, así como una prueba más de la prevalencia de la defensa de los intereses de determinados operadores económicos que impregna toda la Directiva.

A *sensu contrario*, cualquiera que quisiera efectuar operaciones de tratamiento automatizado de datos personales debería garantizar las disponibilidades técnicas y económicas que le permitan afrontar con seriedad y garantía las medidas de seguridad que exige dicho tratamiento. De no ser así, debería prohibírsele tal operación.

Pero las obligaciones en materia de seguridad incumben también a las personas responsables de la realización del tratamiento y, en particular, al encargado del tratamiento.

[51] Sobre este particular, vid. la Decisión del Consejo (92/242/CEE), de 31 de Marzo de 1992, relativa a la seguridad de los sistemas de información, DOCE Nº L 123/19, 8.05.1992.

[52] Cfr. Propuesta de Directiva del Consejo, relativa a la protección de las personas en lo referente al tratamiento de datos personales, COM (90) 314 final - SYN 288, Bruselas, 24 de septiembre de 1990.

Como importante novedad, señalar la obligación a la que se somete al responsable del tratamiento en orden al nombramiento, dentro de su propia estructura y jerarquía organizativa, de un encargado en materia de seguridad técnica y de organización de los tratamientos. Dicho encargado tendrá como principal misión el aseguramiento del cumplimiento de dichas medidas.

Ahora bien, la cuestión está en determinar como se va a verificar este control "interno" de la seguridad; esa dualidad, controlador-controlado, que recae sobre un mismo sujeto.

Asimismo, se incluyen unas previsiones específicas en materia de seguridad cuando el tratamiento sea efectuado por el encargado del tratamiento. Su objetivo es evitar que el hecho de que un tercero efectúe un tratamiento por cuenta del responsable redunde en una menor protección de los interesados.

En este sentido, la realización de un tratamiento por encargo, que deberá constar por escrito o en otra forma equivalente, deberá estar regulada por un contrato u otro acto jurídico entre el encargado del tratamiento con el responsable del mismo. Dos son las menciones inexcusables que deben incorporarse en el referido contrato, y que deben contribuir a delimitar la competencia en materia de seguridad. En primer lugar, que el encargado del tratamiento sólo puede actuar dentro de los límites del contrato con el responsable; en segundo lugar, que las precitadas obligaciones de seguridad, tal y como aparecen diseñadas por las medidas nacionales adoptadas en aplicación de la Directiva, recaen asimismo sobre el encargado del tratamiento.

2.8. *Notificación, control y publicidad de los tratamientos.*

El criterio en materia de notificación debe ser el mismo, independientemente del sector en que se efectúen los tratamientos de datos.

La notificación debe permitir, además de la transparencia de los tratamientos, que la autoridad de control realice un control selectivo de la licitud de los tratamientos.

La obligación de notificación se hace extensiva, a tenor de lo establecido en el *art. 18*, a cualquier tratamiento de datos personales antes de que se lleve a cabo.

Este punto de vista debería incitar a los responsables del tratamiento a prever las medidas necesarias con respecto a las obligaciones que les incumben antes de proceder a la realización de sus tratamientos. Sin embargo, para apreciar el alcance práctico de esta modificación, es conveniente tener en cuenta las disposiciones sobre la simplificación y la exención de la obligación de notificación.

Para garantizar que en el control se tiene en cuenta la realidad global, y en ocasiones, múltiple de los tratamientos efectuados por un responsable de trata-

miento, y para evitar una multiplicación excesiva de las notificaciones, se propone que una sola notificación pueda referirse al conjunto de los tratamientos, repetitivos o no, destinados a la consecución de un fin o de varios fines conexos, relacionados desde el punto de vista del responsable del tratamiento y de los interesados [53].

Pero como señaló el propio Consejo, para responder al deseo de menos burocracia y más eficacia, se ofrece a los Estados miembros posibilidades de excepciones a la obligación de notificación o de simplificación de la notificación [54].

Para elaborar una política común, conviene añadir un criterio que sirva para determinar en qué ámbito resultaría pertinente proceder a la simplificación o a la exención de la obligación de notificación: los tratamientos que no perjudiquen los derechos y libertades de las personas afectadas.

Además, se han permitido excepciones en el caso de que se haya designado a un encargado que se ocupe de las tareas descritas y garantice así que los tratamientos no pueden menoscabar los derechos y libertades de las personas afectadas.

Ahora bien, el beneficio de la simplificación o de la exención de la obligación de notificación no eximirá al responsable del tratamiento de ninguna de las demás obligaciones que emanan de la Directiva [55].

No obstante, otras excepciones pueden establecerse en aquellos casos en que nos encontremos con tratamientos de datos cuya única finalidad sea llevar un registro destinado a facilitar información al público, y siempre que sea un registro abierto al público al general, o pueda ser consultado por toda persona que demuestre un interés legítimo.

Igualmente, los Estados miembros podrán establecer una exención o limitación de la obligación de notificación de los tratamientos, cuando los mismos, referidos a datos "sensibles", sean efectuados por una fundación, asociación u otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical. Consecuencia lógica de la habilitación para tratar datos sensibles que les reconoce el art. 8.2.d), no deben, sin embargo, escapar a toda clase de control. Apelando a la flexibilidad que pretende consagrar la Directiva en esta materia, podrá establecerse un procedimiento simplificado, pero, bajo ningún concepto, una exención total de la obligación de notificación.

[53] A titulo de ejemplo, la Propuesta modificada de Directiva relativa a la protección de las personas..., cit., p. 31, señalaba que sólo debería exigirse una notificación para el conjunto de los tratamientos relativos a la gestión de los préstamos efectuados por un organismo de crédito y destinados a recoger las solicitudes de préstamo, a instruirla, conceder los préstamos, recaudar las cuotas devengadas y estudiar los expedientes conflictivos.

[54] Cfr. Posición Común (CE) Nº 1/95, adoptada por el Consejo el 20 de febrero de 1995..., cit., p. 21.

[55] Tal y como señala su Considerando número 51.

Respecto a los tratamientos no automatizados, se delega en los Estados miembros la facultad de aplicar a los ficheros manuales la posibilidad de una notificación en forma simplificada, adaptándola siempre que se necesario.

Pero la notificación, para asegurar un control eficaz y efectivo por parte de la autoridad de control de los tratamientos, no puede efectuarse en cualquier forma. Si se permitiera que cada responsable del tratamiento incluyera en su notificación aquellas menciones que discrecionalmente considerara relevante, nada se conseguiría, y, además, la pretendida homogeneización que pregona la Directiva se diluiría.

Es por ello que se ha considerado conveniente que en dicha notificación se describan todos los tratamientos previstos y, en particular, tal y como explícitamente señala el *art. 19*, el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante; sus objetivos, los datos o categorías de datos tratados, las categorías de interesados, los terceros o las categorías de terceros a quienes se pueden comunicar los datos, la duración de la conservación de los datos y, en su caso, las condiciones en que se realiza el tratamiento.

La obligación de la notificación de las modificaciones introducidas en los tratamientos que afecten al contenido de la notificación efectuada con anterioridad se recoge para garantizar el seguimiento del control, particularmente importante cuando se modifican los objetivos del tratamiento o cuando puede comunicarse a nuevas categorías de terceros los datos a los que se refiere.

Por otro lado, señalar el acierto de la regulación al tomar en consideración como ciertos tratamientos que pueden comportar riesgos particulares para los derechos y libertades de los interesados deben ser objeto de un dictamen o de una autorización de la autoridad de control, antes de llevarse a cabo [56]. Estos riesgos particulares pueden deberse a la naturaleza de los datos tratados, al alcance del tratamiento o a los objetivos [57].

Los Estados miembros tienen, de acuerdo a lo prescrito por el *art. 20*, la obligación de someter esos tratamientos a un examen previo a su realización por parte de la autoridad de control, o bien por el encargado del tratamiento en cooperación con la autoridad de control. Según su derecho nacional, las autoridades de control podrán emitir un dictamen o dar una autorización una vez realizado el examen previo.

Los Estados miembros podrán llevar también a cabo dicho control previo en el iter parlamentario de una norma, siempre que se defina el carácter del tratamiento y se establezcan las oportunas garantías.

[56] Recoge las Enmiendas número 40, 42, 118 y 119 del Parlamento Europeo.

[57] Tal y como establece su Considerando número 53. Así por ejemplo, tratamientos cuyo objetivo es informar a un tercero de la solvencia de las personas físicas.

Por último, en lo tocante a estas cuestiones, indica el *art. 21* que la autoridad de control tendrá el registro de todos los tratamientos notificados, independientemente del sector al que pertenezca el responsable del tratamiento [58]. Sólo así podrá cumplirse la previsión específica contenida en el punto 1 del precitado artículo, cuando establece la obligación de los Estados miembros de adoptar las medidas necesarias para garantizar la publicidad de los tratamientos.

El registro, que podrá ser consultado por cualquier persona, deberá contener como mínimo las informaciones establecidas en el art. 19, salvo aquellos relativos a las medidas adoptadas para garantizar la seguridad de los tratamientos sin por ello reducir su eficacia. Estas informaciones son las mismas que deberán comunicarse a toda persona que lo solicite, por parte del responsable del tratamiento u otro órgano designado por los Estados miembros, cuando nos encontremos ante tratamientos no sometidos a notificación.

Una excepción se prevé a este régimen general de notificación: tratamientos cuyo fin único sea llevar un registro que éste concebido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo.

2.9. *Flujo transfronterizo de datos.*

La Directiva afirma en su *art. 25* el principio según el cual la transferencia de datos personales de un Estado miembro a un tercer país sólo puede realizarse si dicho país garantiza un nivel de protección adecuado.

En caso contrario, resulta evidente que los esfuerzos llevados a cabo en la Comunidad para garantizar un elevado grado de protección podrían verse anulados por transferencias a terceros países que no garantizaran la suficiente protección.

La libre circulación de datos entre los Estados miembros, que quiere instaurar la presente Directiva, exige la adopción de normas comunes en materia de transferencias a terceros países.

Ahora bien, deberán precisarse los elementos que deben tenerse en cuenta para evaluar la idoneidad de la protección. Se trata de todas las circunstancias que rodean a una transferencia o a una categoría de transferencias, como la naturaleza de los datos, el objetivo de los tratamientos o la normativa vigente en el país en cuestión. Resultará oportuno examinar la normativa general o sectorial, su aplicación real, así como las normas profesionales en vigor, recogidas en los códigos de conducta. La idoneidad de la protección debe evaluarse en relación con una transferencia de datos o con una categoría de transferencias de datos [59].

[58] Recoge las Enmiendas número 37 y 39 del Parlamento.
[59] Recoge la Enmienda número 79 del Parlamento Europeo.

No obstante, cuando la Comisión compruebe que un país tercero no ofrezca un nivel adecuado de protección, lo comunicará a los Estados miembros para que éstos adopten las medidas necesarias para impedir cualquier transferencia de datos personales. La Comisión, ante tal situación, podrá iniciar negociaciones con vistas a solucionar tal eventualidad. A la vista de la legislación interna adoptada o de los compromisos internacionales adoptados por el país tercero, sobre todo a raíz de las referidas negociaciones, podrá la Comisión hacer constar que un país tercero garantiza un nivel de protección adecuado.

Ahora bien, la prohibición de las transferencias a terceros países que no garanticen un grado adecuado de protección viene acompañada por una serie de excepciones, que pueden desvirtuar el contenido de las medidas protectoras.

Las consultas con los sectores implicados demostraron, a juicio de la Comisión y desde la Propuesta del 90, la necesidad de establecer excepciones, en determinados casos, a los principios mencionados [60].

Tomando como base estas "opiniones", el *art. 26* avala que la transferencia a un tercer país que no garantice un grado adecuado de protección pueda efectuarse si el interesado ha dado su consentimiento a la transferencia prevista o si la transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento. En tales casos, el interesado debe estar informado de la realización de la transferencia o de la posibilidad de que se haga a uno o varios terceros países que no garantizan un grado elevado de protección, de modo que pueda decidir si quiere arriesgarse o no a que se lleve a cabo la transferencia en cuestión.

Puede estar también justificada una transferencia a un tercer país que no garantice un grado adecuado de protección cuando resulte necesaria para salvaguarda de un interés público importante o del interés vital del interesado. El objetivo de estas excepciones es facilitar la cooperación internacional o posibilitar la transferencia de datos médicos en circunstancias en que el interesado no pueda expresar su voluntad.

También, cuando sea necesaria para el ejercicio de una acción judicial, o cuando la transferencia se haga desde un registro previsto en la legislación con fines de consulta por el público o por personas con interés legítimo. En el supuesto de

[60] Debido fundamentalmente a las presiones de las grandes multinacionales. Resulta esclarecedor lo contenido en la denominada FICHA DE EVALUACION DE LAS REPERCUSIONES, intitulada REPERCUSION DE LA PROPUESTA EN LAS EMPRESAS Y OTROS ORGANISMOS AFECTADOS, Y EN PARTICULAR, EN LAS PEQUEÑAS Y MEDIANAS EMPRESAS (PYME), donde se señalaba por parte de tales organismos, como una de sus alegaciones, a la Propuesta del 92, la situación que se planteaba ante la imposibilidad de seguir comerciando con un tercer país que no garantice un grado de protección adecuado. Por lo señalado, lo realmente importante era seguir comerciando, al margen de si se vulneran o no los derechos de los ciudadanos. Cfr. Propuesta modificada de Directiva del Consejo relativa a la protección de las personas físicas..., cit., pp. 136-140.

transferencia desde un registro, dicha transferencia no debe afectar a la totalidad de los datos o de las categorías de datos que contenga el mencionado registro [61].

También podrán adoptarse medidas particulares para paliar la insuficiencia del nivel de protección en un tercer país, cuando el responsable del tratamiento ofrezca garantías adecuadas y cuando los demás Estados miembros o la Comisión no se opongan a la medida prevista. En caso de que notificaran su oposición, la Comisión podría tomar las medidas oportunas, en particular prohibir la transferencia, supeditarla a unas condiciones complementarias o entablar negociaciones con el responsable del tratamiento para el que se efectúan las transferencias, con vistas a encontrar soluciones para el conjunto de la Comunidad. [62] Tales garantías irán referidas especialmente al respeto de la vida privada y de los derechos y libertades fundamentales de las personas. En tales supuestos, los Estados miembros podrán autorizar una transferencia de datos. Tales autorizaciones deberán ser comunicadas a la Comisión.

Pero lo que no se indica es a quién competerá, dentro de cada uno de los Estados miembros, la verificación de las garantías aportadas por un responsable del tratamiento. Tal potestad debe otorgarse, sin ningún genero de dudas, a la autoridad de control independiente. Sólo de esta forma podrá evitarse que las controles "gubernamentales" respondan más a intereses políticos, comerciales o económicos, que a lo que deben realmente servir: la defensa de los derechos y libertades fundamentales de los ciudadanos.

2.10. *Recursos Judiciales, Responsabilidades y Sanciones.*

Las legislaciones nacionales deben, conforme al *art. 22*, otorgar la facultad de recurso jurisdiccional a los interesados para permitirles, en su caso, que defiendan no sólo todos los derechos que les reconoce la Directiva. Todo ello sin perjuicio del recurso administrativo previo que podrán interponer ante la autoridad nacional de control.

En lo tocante a la responsabilidad, el *art. 23* hace recaer en el responsable del tratamiento la obligación de reparar el perjuicio causado a cualquier persona por un tratamiento ilícito o una actividad incompatibles con las disposiciones nacionales dictadas en aplicación de la Directiva [63].

El responsable del tratamiento, puede ser eximido de responsabilidad, no obstante, si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor [64].

[61] Tal y como señala su Considerando número 58.
[62] Tal y como señala su Considerando número 59.
[63] Recoge parcialmente la Enmienda número 73 del Parlamento Europeo. No obstante se suprime la referencia a la indemnización de daños y perjuicios, como consecuencia de la responsabilidad, contemplada en la misma Enmienda.
[64] Tal y como señala su Considerando número 55.

Respecto al régimen sancionador, los Estados miembros establecerán las sanciones adecuadas, conforme al *art. 24*, para los casos de incumplimiento de las disposiciones adoptadas en ejecución de la Directiva [65].

2.11. *Códigos de Conducta.*

Las experiencias de algunos Estados miembros al respecto ha llevado a incluir en la Directiva, concretamente en su *art. 27*, una disposición encaminada a fomentar la elaboración de códigos de conducta a escala nacional y comunitaria.

Los códigos pueden constituir un elemento positivo de cara a una buena aceptación de la normativa aplicable, dado que los sectores profesionales se ven obligados a participar de manera directa en su aplicación.

Responden a las siguientes características:

a. La iniciativa de su elaboración y su redacción son responsabilidad exclusiva de los sectores profesionales, independientemente de los estímulos que puedan recibir de las autoridades públicas. En este sentido se manifiesta la Directiva al señalar que: "Los Estados miembros *alentarán* la elaboración de códigos de conducta destinados a contribuir, en función de las peculiaridades de cada sector a la correcta aplicación de las disposiciones..." [66].

b. Su alcance se limita a aplicar o desarrollar la normativa aplicable, pero no a establecer excepciones.

c. Su efecto no es vinculante para los terceros ni para los organismos jurisdiccionales, que siempre pueden hacer prevalecer la normativa que están encargados de aplicar. No obstante, las asociaciones profesionales y demás organizaciones podrán someter los proyectos de Códigos, o sus modificaciones o prórrogas, a examen de las autoridades de control.

Como es natural puede ocurrir que la autoridad pública y, en particular, los órganos legislativos, recojan por cuenta propia los Códigos elaborados por los sectores profesionales para darles un carácter vinculante desde el punto de vista legislativo.

[65] La redacción del artículo no recoge no obstante las consideraciones apuntadas por el Parlamento Europeo en su Enmienda número 77, y que rezaba del siguiente tenor: "Los Estados miembros preverán en su legislación la aplicación de sanciones disuasivas, aplicables a las autoridades y organizaciones regidas por el Derecho público, así como a otras personas naturales o jurídicas, a fin de garantizar el cumplimiento de las normas adoptadas en aplicación de la presente Directiva."
[66] Punto 1. del art. 18. A nivel comunitario, y referido a la regulación jurídica de Internet, vid. Propuesta de Recomendación del Consejo relativa a la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información, COM(97) 570 final, 97/0329 (CNS), 18.11.97, especialmente su "Anexo: líneas directrices comunes, para la aplicación, al nivel nacional, de un marco de autorregulación para la protección de los menores, de la dignidad humana en los servicios audiovisuales y de información en línea".

Se encarga a la autoridad de control que compruebe, entre otras cuestiones, la procedencia de los códigos con respecto a las disposiciones nacionales adoptadas en virtud de lo dispuesto en la Directiva, y recoja, si lo considera conveniente, las observaciones de los interesados o de sus representantes [67].

Respecto a los Códigos comunitarios, la competencia otorgada a la autoridad de control con respecto a los códigos nacionales, es de la misma naturaleza que la otorgada al Grupo de Protección comunitario. Para informar al público en general, la Comisión podrá publicar en el DOCE los Códigos, conjuntamente con el dictamen del Grupo.

2.12. *Autoridad de control y Grupo de protección de las personas en lo que respecta al tratamiento de datos personales.*

La Autoridad de control, cuya característica esencial debe ser la independencia [68], se articula en la Directiva en su *art. 28*, y de acuerdo a los siguientes postulados:

'a) Nombramiento de la autoridad de control. Cada Estado miembro dispondrá que, para tener en cuenta particularmente la estructura federal de algunos Estados miembros, una o más autoridades de control se encarguen de vigilar la aplicación de las disposiciones adoptadas en aplicación de la Directiva [69].

b) Poder de la autoridad de control. Se dota a estas autoridades de medios de investigación y de intervención con respecto a los responsables de los tratamientos y bajo el control de las autoridades judiciales. Asimismo, se prevé la consulta sistemática de las autoridades de control con motivo de la elaboración de medidas reglamentarias o administrativas nacionales.

La facultad de intervención tiene por objeto permitir a la autoridad de control que recabe de los responsables del tratamiento los datos necesarios para el cumplimiento de su cometido. Esta competencia se manifiesta en particular en el acceso a los datos que son objeto de tratamiento. Para respetar los derechos de las personas sometidas al control de la autoridad, estas prerrogativas deben utilizarse respetando estrictamente la confidencialidad que les concede a los datos en cuestión el Derecho nacional [70].

Para que la autoridad de control pueda cumplir su cometido, resulta esencial que disponga de un poder efectivo de intervención: formular dictámenes y garantizar una publicidad adecuada de los mismos, poder de ordenar el bloqueo o la supresión de los datos, de prohibir un tratamiento, dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a Parlamentos u otras instituciones políticas nacionales [71].

De igual forma, se dota a la autoridad de control de capacidad procesal; es decir, del poder de recurrir a la autoridad judicial cuando constante la existencia de infracciones a las disposiciones nacionales de aplicación de la Directiva. Esta facultad se desprende lógicamente de la facultad de investigación.

Resultaría extraño que una autoridad encargada de proteger a las personas no pudiera recurrir a la autoridad judicial en caso de que constatara una infracción. Esta posibilidad se desdobla en una doble perspectiva: 1. si la autoridad de control es la encargada de la protección de las personas en lo que respecta a las informaciones que les conciernen, debe tener, consecuentemente, la posibilidad de poner los hechos lesivos afectantes a las mismas en conocimiento de la autoridad judicial competente; y, 2. el derecho de cualquier persona a presentar una denuncia ante la autoridad de control, de modo que dicha denuncia pueda, por su intermedio, llegar ante la autoridad judicial.

No obstante, el panorama mostrado, los poderes de intervención de dichas autoridades de control son descritos, siguiendo lo señalado por el propio Consejo, de forma indicativa con el fin de conceder a los Estados miembros la flexibilidad necesaria en este ámbito [72].

c) Presentación de informes anuales. La autoridad de control puede presentar de manera periódica un informe sobre sus actividades, donde se haga hincapié en los problemas planteados por la aplicación de las disposiciones legislativas y se indiquen los nuevos derroteros que deberán seguirse.

Se han introducido también, por último, precisiones sobre la cooperación entre las autoridades de control en materia de flujos transfronterizos [73].

En lo afectante al Grupo de Protección de las Personas frente al Tratamiento de Datos Personales, éste tendrá un carácter consultivo e independiente [74]. Su estructura puede sistematizarse, de acuerdo a lo regulado en el *art. 29*, siguiendo el siguiente esquema:

1. Presidencia del Grupo: el Grupo elige un presidente por un mandato prorrogable de dos años de duración.

[67] No se recoge lo señalado por la Enmienda número 72 del Parlamento Europeo, referente a que los Códigos se elaborarán sobre la base de los derechos fundamentales que se contemplan en las Constituciones de los Estados miembros y del Convenio Europeo de Derechos Humanos.
[68] Recoge las Enmiendas número 84, 85, 86 y 87 del Parlamento Europeo.
[69] Recoge la Enmienda número 84 del Parlamento.
[70] El apartado 7 de este artículo establece: "Los Estados miembros dispondrán que los miembros y agentes de la autoridad de control, estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso".
[71] Recoge, sustancialmente, la Enmienda número 86 del Parlamento.
[72] Cfr. Posición Común (CE) Nº 1/95, adoptada por el Consejo el 20 de febrero de 1995..., cit., p. 24.
[73] Punto 6 del art. 28.
[74] Recoge las Enmiendas número 88 y 128 del Parlamento.

2. Composición del Grupo: se limita la composición del Grupo a los representantes de las autoridades de control nacionales. En caso de que algunos Estados miembros hicieran uso de la facultad de que disponen de nombrar a varias autoridades de control, se establece que la representación de las autoridades de los Estados miembros en cuestión del Grupo comunitario sea común.
3. Adopción de decisiones: el Grupo adoptará sus decisiones por mayoría simple de los representantes de las autoridades de control. El Grupo aprobará, asimismo, su reglamento interno.

En lo atinente a sus funciones, siguiendo lo establecido en el *art. 30*, pueden señalarse las siguientes:

— dictaminar sobre la ejecución de las disposiciones nacionales tomadas para la aplicación de la Directiva;
— dictaminar sobre el nivel de protección existente en la Comunidad y en los países terceros;
— asesorar a la Comisión sobre las medidas que deben tomarse, en el curso de un proceso legislativo comunitario, para salvaguardar los derechos y libertades de las personas de las personas físicas respecto a sus datos personales;
— dictaminar sobre los Códigos de conducta comunitarios,
— posibilidad de formular recomendaciones por iniciativa propia sobre cualquier cuestión relacionada con la protección de los datos personales en la Comunidad.

El Grupo elaborará un informe anual sobre el estado en que se encuentre la protección de los datos personales en la Comunidad y en los terceros países. Este informe, que será transmitido al Parlamento Europeo, al Consejo y a la Comisión, será publicado.

2.13. *Limitaciones y excepciones.*

La inclusión de este apartado en nuestras consideraciones finales sobre la Directiva no responde, ni a un olvido involuntario, ni a que esta materia presente una dificultad especial para encontrarle una emplazamiento adecuado. Responde a un intento deliberado, y por ello estrictamente personal, por intentar mostrar cual puede ser la efectiva aplicación de las previsiones de la Directiva.

La apelación en numerosas disposiciones legislativas a conceptos tales como "orden público", "seguridad nacional", etc., no supone desgraciadamente ninguna novedad. Y de manera especialmente profusa abundan en los textos referentes a los derechos y libertades fundamentales; utilizándose habitualmente como criterios enmascaradores de políticas restrictivas o limitativas del reconocimiento y efectividad de aquéllos.

Sucede aquello señalado por Pérez Luño, cuando escribe:

> "En su escrito sobre *El 18 Brumario de Luis Bonaparte* Karl Marx denunció refiriéndose a la Carta constitucional francesa de 1848, que: «Cada artículo de la Constitución contiene su propia antítesis, su propia Cámara alta y baja. En la frase general la libertad, en su explicación la anulación de la libertad. Por ello, mientras formalmente se respetase la libertad, aunque por vía legal se impidiera su ejercicio, la libertad quedaba intacta por más que se negase su significación común y popular»"[75].

Algo similar ocurre con las previsiones "garantistas" que incorpora la Directiva en lo referente a la protección de los datos personales. Tras desglosar a lo largo de su articulado todo un elenco de prevenciones, controles y "defensas" tendentes a la protección de los derechos y libertades de los ciudadanos, incluye en su *art. 13*, de manera disimulada (a modo de intento de pasar desapercibido) toda una batería de excepciones, de vulneración de las garantías propugnadas; en definitiva, de la consagración de la más absoluta arbitrariedad estatal para limitar, e incluso anular, los derechos y ~~libertades más elementales~~ de los ciudadanos.

No es que estemos abogando por que los Estados democráticos no puedan servirse de medidas represivas para combatir los desmanes de criminales y terroristas, los fraudes, el narcotráfico, etc. Pero ello no supone poner a todos los ciudadanos bajo la mirada de la sospecha, convertirlos en potenciales "enemigos", perseguirlos y controlarlos de manera clandestina vulnerando su libertad, e incluso su dignidad.

Precisamente por ser democráticos, los Estados que así se autocalifican, deben garantizar a sus ciudadanos una vida en libertad y respeto. Sólo a los que infringen las normas, a los que intentan someter al resto del pueblo a sus asesinos designios, deben aplicarse esas medidas. La persecución y prevención de determinados delitos, aún tomando en consideración su enorme importancia para la conservación de la convivencia democrática, no debe ser tampoco una habilitación para el "todo vale".

Volviendo a lo señalado por el art. 13, indicar como corresponde a los Estados miembros ~~decidir en qué medida~~ deben incluir excepciones en su legislación nacional relativa a la protección de datos. Dichas medidas quedan así al exclusivo arbitrio y oportunidad de los Estados miembros, que podrán usar de ellas en todo momento y en las circunstancias que consideren procedentes.

Pero además, esta "autonomía" estatal puede suponer una grave lacra para el desarrollo de políticas comunitarias homogéneas, al propiciar enfoques divergentes, interpretaciones contrarias, e incluso, soluciones diferentes para la considera-

[75] Cfr. PEREZ LUÑO, A.E., Derechos Humanos, Estado de Derecho y Constitución, 5ª edic., Tecnos, Madrid, 1995, p. 266.

ción de un mismo problema. Todo ello con grave quiebra de la seguridad jurídica que debe acompañar a los ciudadanos en el reconocimiento y defensa de sus derechos.

Las medidas legales restrictivas que se adopten pueden suponer la inaplicación, en este ámbito, de las disposiciones de la Directiva referidas a: principios relativos a la calidad de los datos, información y derechos del interesado y publicidad de los tratamientos.

Como se observará, las excepciones afectan a sectores capitales, vertebradores de la Directiva e indispensables para ese elevado nivel de protección de las personas en lo tocante a los datos personales a ellas referidos, y que con tanto énfasis propugnaba en su art. 1. Pero si ahondamos más en una dimensión práctica, ante tales derogaciones, ¿que queda a los ciudadanos para la defensa de sus derechos e intereses?; ¿debemos permanecer impasibles y someternos incondicionalmente al Estado?. Otras muchas cuestiones nos asaltan de manera instantánea, y contribuyen a nuestro desencanto ante el panorama que se nos ofrece. Todo lo que incorporaba la regulación comunitaria con un carácter delimitador - y claramente protector - queda de un plumazo desvirtuado, eliminado; en definitiva, dinamitado.

Y aunque se indica que estas medidas se limitan a aquellas que son necesarias para la salvaguarda de determinados valores, la relación de los mismos es ciertamente exhaustiva. Claro elenco de conceptos jurídicos indeterminados, van especialmente referidos, siguiendo lo señalado por la Comisión en su Propuesta del 90 [76], a:

a) la seguridad del Estado. Por tal hay que entender la protección de la soberanía nacional contra amenazas internas y externas.
b) la defensa. Deberán incluirse bajo esta mención todos los aspectos relativos a la protección militar del Estado.
c) la seguridad pública. Comprende todas las funciones policiales de los órganos del Estado, incluida la prevención del crimen.
d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas.
e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales. Se refiere a todas las medidas de política económica y a los medios de financiación de las políticas de un Estado miembro o de la Comunidad. No obstante, se ha omitido la referencia contenida en la Propuesta del 90, cuan-

[76] Cfr. Propuesta modificada de Directiva del Consejo relativa a la protección de las personas..., cit., p. 25.

Sirva, además de como *excursus*, señalar que la propia Directiva, señala en su *Considerando 11*, "que los principios de la protección de los derechos y libertades de las personas... precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa...". La Directiva, por lo tanto, no asume el Convenio 108, sino que lo precisa y amplia. Su actividad normativa se aparta así de dicha regulación, superponiéndose a la misma y superándola. La Comunidad, embarcada en la tarea de crear una identidad propia, no puede asumir sin más un elemento jurídico "extraño" a su propio sistema normativo, lo cual le haría depender de otros presupuestos ajenos a su propia configuración y objetivos. Tal vez por ello, y pese a los numerosos requerimientos hechos por la propia Comisión Europea, la Comunidad no se haya adherido, en cuanto tal, al referido Convenio del Consejo de Europa. Ha optado por elaborar una política propia y adecuada a sus concretas necesidades y exigencias comunitarias.

Estas son las definiciones recogidas:

a) *Datos personales.* Su naturaleza es la de una definición de carácter general, con objeto de abarcar todos los datos que pueden relacionarse con una persona física [23].
Una persona puede identificarse bien de manera directa, mediante un nombre, bien de manera indirecta, mediante un número de teléfono, el código de su coche, de la Seguridad Social, del pasaporte o mediante un haz de rasgos distintivos, que permita aislarla de un grupo (edad, cargo desempeñado, dirección, etc.) La definición comprende también datos como la imagen y la voz, las huellas dactilares y las características genéticas.

b) *Tratamiento de datos personales.* Se propugna un ámbito de aplicación amplio, que permita garantizar la protección de las personas [24], puesto que comprende los datos desde su recogida hasta su supresión, pasando por su organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación (por transmisión), difusión o cualquier forma que facilite el acceso a los mismos [25], cotejo o interconexión, así como su bloqueo, supresión o destrucción.

c) *Fichero de datos personales.* Comprende tanto los ficheros automatizados como los no automatizados. Permite, en lo referente a los tratamientos de datos no automatizados, circunscribir el ámbito de aplicación de la Directiva a los datos estructurados para facilitar el acceso y la búsqueda de aquéllos que se refieran a personas físicas. Quedan excluidos los datos personales que no están organizados para su utilización en relación con los interesados.

[23] Recoge la Enmienda número 12 del Parlamento Europeo.
[24] Recoge la Enmienda número 15 del Parlamento Europeo.
[25] Recoge la Enmienda número 16 del Parlamento Europeo.

Como señala su *Considerando 15*, "los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata".

d) *Responsable del tratamiento.* El objetivo principal de la Directiva es regular la utilización de los datos en función de los fines a que se destinan.
Se tratara de la persona responsable, en última instancia, de las opciones escogidas a la hora de determinar y llevar a cabo los tratamientos, y no de las personas que efectúan las operaciones de tratamiento de acuerdo con las instrucciones del responsable, razón por la cual se indica que es el responsable quien decide "los objetivos" del tratamiento. El responsable del tratamiento puede tratar los datos por sí mismo o hacer que los traten los miembros del personal a su cargo o el agente tratante, persona jurídicamente diferente del responsable pero que actúa por cuenta de él.

e) *Encargado del Tratamiento.* También denominado Agente tratante [26], será la persona, física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

f) *Terceros.* No se consideran terceros ni el interesado ni el responsable del tratamiento ni las personas autorizadas a tratar los datos bajo su autoridad directa o actuando por cuenta propia.
Respecto a la consideración de terceros, la Propia Comisión en su Propuesta del 92 estableció algunas precisiones, respecto a las entidades y empresas de gestión y actividades descentralizadas, que puede ser de interés tener en consideración. Así, las personas que trabajan en otra empresa, aunque forme parte del mismo grupo o sociedad de cartera, deberían considerarse por lo general terceros.
En cambio, las sucursales bancarias que efectúan tratamientos para la gestión de la clientela y que están situadas bajo la autoridad directa de la sede no deberían considerarse terceros. Lo mismo puede decirse de los agentes de seguros; por el contrario, en lo que respecta a los representantes de seguros, la situación puede diferir en cada caso [27].

g) *Destinatario.* Entiéndase por tal, la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. Equiparable a la figura de un "cesionario" de

[26] Tal era la denominación otorgada por el Parlamento Europeo en su Enmienda número 18 al texto de la Propuesta modificada de Directiva del 92.
[27] Cfr. Propuesta modificada de Directiva..., cit., p. 11.

datos personales, fue introducida en la Posición Común del Consejo, ya "que es útil para garantizar la transparencia de los tratamientos con respecto a las personas afectadas" [28].

h) *Consentimiento del interesado.* En la propuesta inicial del año 90 figuraba en el capítulo dedicado a los derechos de las personas.
Este hecho provocó graves objeciones al texto de la Directiva. Varios sectores profesionales dedujeron que cualquier tratamiento exigía el consentimiento previo del interesado, lo cual suponía una importante "traba" para el desarrollo de sus actividades económicas o mercantiles. Ante esta situación se optó por incluirlo, como veremos más adelante, como un requisito más que legitima un tratamiento automatizado de datos; pero sin concederle el valor preeminente que debe tener, como manifestación de la autodeterminación personal inherente a toda persona.
El consentimiento aparece conceptuado como toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que la conciernan. Desglosemos las características que deben adornar ese consentimiento.

1. El consentimiento debe ser libre e informado.

El consentimiento libre excluye todas aquellas manifestaciones de voluntad obtenidas bajo algún genero de violencia física o psíquica que coarte la libre determinación del sujeto afectado.

Para que el interesado pueda apreciar los riesgos y las ventajas del tratamiento de datos que le conciernen y ejercer los derechos que le reconoce el artículo 12 de la Directiva (rectificación, supresión, bloqueo), el consentimiento deberá darse disponiéndose de la información suficiente; razón por la cual el responsable del tratamiento debe comunicar al interesado las informaciones que requiere, tal y como se deduce del *art. 10.*

2. El consentimiento del interesado debe ser específico, es decir, que debe referirse a un tratamiento de datos en concreto, que conciernan al interesado y que lleve a cabo un responsable determinado con fines determinados.

Resulta sorprendente, por otro lado, como la Directiva ha omitido la previsión contenida en la Propuesta del 92, y que otorgaba al interesado la posibilidad de revocar su consentimiento en cualquier momento. Exigencia ineludible de libertad personal, supone una facultad que, no por obvia, debería indicarse de manera expresa en el texto.

[28] Cfr. Posición Común (CE) Nº 1/95, adoptada por el Consejo el 20 de febrero de 1995, con vistas a la adopción de la Directiva 95/../CE del Parlamento y del Consejo, de..., 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; DOCE, Nº C 93/22, 13.4.1995.

2.3. *Ambito de aplicación y Derecho nacional aplicable.*

La Directiva adopta en su *art. 3* criterios diferentes para delimitar el ámbito de aplicación de la Directiva, en función de que los datos sean o no objeto de tratamiento automatizado: sólo es aplicable al tratamiento no automatizado de datos si éstos están contenidos en un fichero. La Directiva se aplica a cualquier tratamiento automatizado de datos, aunque dichos datos no estén contenidos en un fichero.

Se aplica a datos personales estructurados, bien por su organización en un fichero manual, bien mediante un tratamiento informático. Ahora bien, cabe plantearse que ocurrirá con los datos personales aislados objetos de un proceso de interconexión.

Se hace referencia a los tratamientos automatizados "completamente o en parte" para recalcar que un tratamiento constituye un todo, incluso aunque sólo esté informatizada una parte de dicho tratamiento.

De este modo, los principios que emanan de la Directiva no dependen de una tecnología u organización técnica especiales. La atención se centra en los datos utilizados y en el conjunto de operaciones a que se refieren, en función de los fines perseguidos.

Ahora bien, este amplio régimen de aplicación, queda desvirtuado gravemente cuando se incorporan unas generosas, y en la mayoría de los casos indefinidas, excepciones a los principios señalados anteriormente. La defensa de unos intereses más o menos difusos permiten que determinados tratamiento automatizados de datos personales quedan exceptuados del acatamiento a los principios protectores que pretende articular la Directiva. Estas excepciones se refieren a las siguientes categorías de datos:

a) Los tratamientos efectuados para ejercer actividades que no figuran en el ámbito de aplicación del Derecho Comunitario; tales como las previstas por las disposiciones de los Títulos V y VI del Tratado de la Unión Europea. Es decir, aquellas referentes a la cooperación en los ámbitos de la Justicia e interior, así como a las referidas a la Política exterior y de seguridad común. La naturaleza intergubernamental de estas políticas las aparta del proceso ordinario de aplicación y control al que está sometido el Derecho comunitario, conceptuándose, como hace la propia Comisión, como una de las nuevas formas de actuación de que se ha dotado la Unión para "completar las Comunidades Europeas" [29]. El Acuerdo de Schengen, como veremos posteriormente, es un magnífico ejemplo de como "se completa" la política comunitaria.

[29] Cfr. Parlamento Europeo. CONFERENCIA INTERGUBERNAMENTAL 1996., cit., p. 51.

El ámbito de aplicación se define, por tanto, en relación con el ámbito de aplicación del Derecho Comunitario, para permitirle evolucionar conjuntamente con éste.

b) Derivado de la excepción *ratione materiae* anterior, se precisa aún más señalando que *en cualquier caso* las disposiciones de la Directiva tampoco se aplicarán a un 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.
La inclusión de este generoso régimen de excepciones, tomando como basamento todo un elenco de conceptos jurídicos indeterminados, supone una grave quiebra en el sistema de garantías que articula la Directiva, y unas inmensas posibilidades para los Estados de tratar un gran número de datos personales sin someterse a control o verificación alguna.

c) Utilización de datos en el ejercicio de actividades exclusivamente personales o domésticas (v.g. agendas electrónicas) [30].

Por su parte, el *art. 4* fija los criterios necesarios para determinar cuál es la legislación nacional aplicable a los tratamientos que entran dentro del ámbito de aplicación de la Directiva, con objeto de evitar:

1. por una parte, que el interesado carezca de protección, en particular debido a una elusión de la legislación;
2. por otra, que un mismo tratamiento se vea sometido a la aplicación de varias legislaciones nacionales [31].

La localización de un fichero o de un tratamiento serán a menudo imposibles de determinar. En efecto, éstos últimos podrían localizarse en múltiples puntos, estar repartidos entre varios Estados miembros, especialmente en el caso de las bases de datos y de las redes, fenómenos en constante expansión.

El derecho aplicable se define por referencia al lugar de establecimiento del responsable del tratamiento. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple ellos las obligaciones previstas por el Derecho nacional aplicable.

En caso de que el responsable del tratamiento no esté radicado en el territorio de la Comunidad, pero utilice medios, automatizados o no, para efectuar un trata-

[30] Recoge la Enmienda número 22 del Parlamento Europeo.
[31] Cfr. CARRASCOSA GONZALEZ, J., "Protección de la intimidad y tratamiento automatizado...", cit., pp. 437-439.

miento, y localizados en el territorio de un Estado Miembro, el derecho aplicable será el del Estado en cuyo territorio están localizados dichos medios. Se exceptúan los supuestos en que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad.

El responsable del tratamiento deberá nombrar a un representante radicado en dicho territorio, que quedará subrogado en sus derechos y obligaciones.

Será a este representante a quien le incumba la obligación de notificación. De la misma manera, cualquier información de los interesados acerca del responsable del tratamiento prevista por la Directiva deberá completarse mediante una información sobre su representante; obligación establecida en los *arts. 10.1* y *11.1.*

Debido a la elección del criterio del establecimiento del responsable del tratamiento, el desplazamiento temporal de un fichero no deberá modificar en ningún caso el Derecho aplicable.

2.4. *Condiciones generales para la licitud del tratamiento de datos personales.*

El capítulo II de la Directiva recoge el conjunto de principios, derechos y obligaciones que determinan la licitud de los tratamientos efectuados.

El *art. 5* establece que los Estados Miembros dispondrán que los tratamientos de datos sólo serán lícitos cuando se ajusten a lo dispuesto en el Capítulo II, que se constituye como una unidad.

Los Estados Miembros precisarán en su legislación las condiciones en que son lícitos los tratamientos. Ahora bien, siempre atemperándose y con inexcusable observancia de lo señalado en este Capítulo; que se configura de esta forma como el referente imprescindible para llevar a cabo un tratamiento automatizado de datos personales.

Dos cuestiones, no obstante, deben distinguirse dentro de esta genérica previsión normativa:

a) Principios relativos al tratamiento de datos.

El *art. 7* agrupa las condiciones de legitimidad necesarias para proceder a un tratamiento de datos personales. Es decir, nos señala en que circunstancias o supuestos podrá procederse a un tratamiento tal. Tales circunstancias se refieren especialmente a:

1. El *consentimiento* ya no se considera el criterio principal ni se establecen excepciones, sino que se convierte en una condición más. El consentimiento debe haberse otorgado de manera inequívoca. Lo cual entendemos implica

la necesidad de un consentimiento informado, en lo material, y concluyente, en su forma de manifestación formal.

2. El tratamiento de datos personales es necesario para la ejecución de un contrato en el que el interesado sea parte. Ahora bien, deben ir referidos exclusivamente a aquellos datos *estrictamente* necesarios para la articulación de una correcta relación laboral.
   Se ha incluido también la referencia a "medidas precontractuales", para contemplar la adopción de medidas anteriores a la creación de una relación contractual, adoptadas a petición del interesado.

3. Tratamiento realizado a raíz de una obligación jurídica a la que esté sujeto el responsable del tratamiento. Dada la naturaleza de la Directiva, con una amplia habilitación a los Estados miembros para articular las medidas que establece, entendemos que dicha obligación podrá venir impuesta tanto por el Derecho nacional, como por el Derecho Comunitario.
   Asimismo, cuando el tratamiento de datos personales sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos.

4. Se comprenden igualmente los casos en que el interesado tenga un interés vital en el tratamiento de sus datos personales, pero no esté en condiciones de dar su consentimiento. Como señala la propia Directiva en su *art. 8.2.a)*, referente al tratamiento de los llamados datos sensibles, en aquellos supuestos en que el interesado esté física o jurídicamente incapacitado para dar su consentimiento. Sin embargo, ¿ que debe entenderse por "interés vital" en el tratamiento de datos ?.
   Si el Derecho Civil tiene establecido el nombramiento de un representante legal en los supuestos en que se decreta la incapacidad de una persona [32], no podría quizás haberse establecido de manera análoga, y para estos supuestos de incapacidad, la designación de una especie de "sustituto legal", que ejerciera los derechos reconocidos al interesado.

5. Puede resultar necesario para la satisfacción de importantes intereses legítimos del responsable del tratamiento o del/os tercero/s [33]. Y siempre que no prevalezcan el interés o los derechos y libertades fundamentales del interesado. Por otro lado, acertadamente se ha suprimido la referencia a los datos provenientes de fuentes generalmente accesibles para el público. La Comisión constató que, en determinados casos, algunas fuentes de acceso público general pueden contener datos personales especiales. Además, en la mayoría de los casos, los datos han sido tratados con fines específicos y, por consi-

[32] Cfr., para el ordenamiento jurídico español, los arts. 222 a 285 de nuestro Código Civil.
[33] Recoge en parte la Enmienda número 32 del Parlamento Europeo.

guiente, no deberían utilizarse con otro objeto sin tener en cuenta las demás disposiciones de la Directiva [34].

b) Principios relativos a la calidad de los datos.

Las disposiciones del *art. 6* recogen, con ciertas modificaciones, los principios del Convenio 108 del Consejo de Europa y de la mayor parte de las legislaciones nacionales de protección de datos.

Como primer requisito, el tratamiento de datos personales deberá efectuarse de *forma lícita y leal*. Esta disposición comprende la recogida. Se excluye en particular la utilización de aparatos ocultos para obtener datos subrepticiamente y sin conocimiento del interesado, en concreto mediante escuchas telefónicas y otros medios, etc. Esta disposición prohíbe asimismo que los responsables de los tratamientos realicen o utilicen tratamientos clandestinos sobre datos personales.

La letra b) enuncia el principio de la *determinación de la finalidad* de la recogida de datos. Sólo se podrán conservar datos personales para fines determinados, explícitos (lo cual implica que deberá informarse a los interesados acerca de la finalidad de los tratamientos) y legítimos.

El objeto de la recogida de datos personales debe determinarse, esto es, la finalidad de la recogida y utilización de los datos deberá definirse de la manera más precisa posible. Una definición o descripción vagas del objeto del tratamiento no será acorde con el principio de la definición de la finalidad. Es necesario precisar la finalidad del tratamiento antes de efectuar la recogida de los datos. En el supuesto de que los datos se recaben del propio interesado, la finalidad deberá haberse determinado antes de que se realice la recogida.

También se establece que una modificación posterior de la finalidad de un tratamiento sólo será legítima en la medida en que sea compatible con la finalidad inicial.

Sin embargo, esta posibilidad no supone más que una "puerta falsa" para subvertir las previsiones de la Directiva y obviar la necesidad de determinación de los tratamientos. La apelación a la compatibilidad de los objetivos, amplía considerablemente las posibilidades de tratamientos de datos personales, al margen de las garantías establecidas por la Directiva. El objetivo de los tratamientos debe quedar clara y perfectamente predeterminado, para garantizar así a los ciudadanos el pleno ejercicio de los derechos reconocidos en la Directiva. Si los "afectados" desconocen el ámbito material y la extensión del tratamiento, difícilmente podrán ejercitar sus derechos de acceso, rectificación o cancelación.

[34] Recogida en la antigua letra b) del apartado 1 del artículo 8 de la Propuesta del 90. Cfr. Propuesta modificada de Directiva.., cit., p. 17.

Además, la compatibilidad entre las finalidades no exime del riesgo de un uso indebido de los datos. Una cosa será la finalidad que se dé a los datos recabados, y otra muy distinta, el uso que de esos datos se haga amparándose en dicha finalidad.

Por otro lado, el responsable del tratamiento será el que determine "*a posteriori*" dicha compatibilidad, con lo cual tal garantía queda vacía, pues será ilógico pensar que el responsable vaya a "autocensurarse". La compatibilidad que en su caso realice el responsable del tratamiento se acomodará más a los intereses particulares del momento o de la operación en curso, que a la finalidad primigenia. La labor asignada a las Autoridades de control debería incluir entre sus actuaciones el control de tales "compatibilidades".

Por último, no se consideran incompatibles los tratamientos que, apartándose de la finalidad previamente determinada, tengan por objeto fines históricos, estadísticos o científicos. Sobre esta cuestión volveremos posteriormente al abordar la posibilidad establecida también en la propia Directiva de una conservación "ilimitada" de esta categoría de datos.

Los datos deberán ser *adecuados, pertinentes y no excesivos* con relación a los fines para los que se recaben y traten. Esto implica que la naturaleza de los datos debe corresponderse con el objetivo perseguido.

Igualmente, habrán de ser *exactos y, cuando sea necesario, deben actualizarse*. En caso de que hubiera datos incorrectos o incompletos con respecto a los fines para los que fueron recogidos, se prevé que se supriman o rectifiquen.

Respecto a la duración máxima de conservación de datos personales, su conservación en una forma que permita la identificación del interesado sólo queda autorizada durante el período que sea necesario para alcanzar los fines para los que se registraron los datos.

Lo que si resulta paradójico es que quien mantiene la posibilidad de identificación de los datos, sea quien también, con relación a una finalidad, o incluso, a finalidades potenciales, determine libremente la "necesidad" de conservarlos de esa forma. Hubiera sido más conveniente establecer un "sistema de plazos máximos" dentro del cual pueda mantenerse dicha identificación.

Por otro lado, en determinados casos y tras cierto plazo, si un tratamiento ha dejado de ser un instrumento de gestión, puede ser necesario conservarlo por motivos históricos, estadísticos o de investigación científica.

De conformidad con el dictamen del Parlamento [35], los Estados Miembros podrán prever garantías apropiadas para los datos archivados por motivos histori-

[35] Recoge la Enmienda número 60 del Parlamento.

cos, estadísticos o científicos, para conciliar el principio estricto de la finalidad con el *"derecho al olvido"* y, por otra parte, satisfacer las exigencias de la investigación.

Ahora bien, la cuestión a dilucidar es establecer cual será el criterio, teniendo en cuenta que deberá operarse con un carácter "anticipador", mediante el que podrá determinarse la "futura" relevancia histórica de un determinado dato. Todos los datos son susceptibles de coadyuvar a la comprensión de determinados procesos históricos, y por tanto, todos deberían conservarse. La introducción de esta posibilidad de conservación en la Directiva, aunque formulado con un inicial propósito loable, será foco de no pocos conflictos y tensiones.

Por último, de manera congruente con lo regulado, el apartado 2 del art. 6 obliga al responsable del tratamiento a garantizar el respeto de las disposiciones sobre la calidad de los datos establecidas en el apartado 1.

2.5. *Los derechos de la persona afectada.*

Señala Lucas Murillo de la Cueva, como el contenido típico del derecho a la autodeterminación informativa está integrado por las diferentes facultades y poderes de control que se reconocen a sus titulares sobre la información personal que les afecte [36]. Dentro de la estructura de la Directiva, estas facultades y poderes pueden agruparse en torno a las siguientes categorías de derechos, que a continuación exponemos.

a) Derecho de Información.

Recogido en el antiguo art. 10 de la Propuesta del 92, se concretaba en el derecho del afectado a recibir información sobre la existencia de un tratamiento. Formulado como tal derecho, su ejercicio se difería, en una incorrecta e incoherente regulación, a una solicitud previa del interesado al responsable del tratamiento.

Las obligaciones relativas a la información de la persona afectada se han hecho en la Directiva más flexibles. Ello se debe, como sostiene el propio Consejo, a la necesidad de tener en cuenta la gran diversidad de circunstancias en las que pueden realizarse tales tratamientos [37]. Resulta cuestionable, sin embargo, que tras establecer la obligación general de información por parte del responsable del tratamiento, se excepcione el régimen general, basándose en unas causas indeterminadas. El problema estribará en la determinación de tales circunstancias, así como en la concreción de las personas u organismos encargados de tal apreciación en el momento de la recogida.

[36] Cfr. LUCAS MURILLO DE LA CUEVA, P., Informática y protección de datos personales, Centro de Estudios Constitucionales, Madrid, 1993, p. 55.

[37] Cfr. Posición Común (CE) Nº 1/95, adoptada por el Consejo el 20 de febrero de 1995..., cit., p. 23.

Ahora bien, la omisión explícita de tal derecho nos parece de todo punto intolerable, por cuanto supone el no reconocimiento de un derecho fundamental, base imprescindible del derecho a la autodeterminación informativa, y garantía primigenia de los ciudadanos para la protección de los datos personales que le conciernen. Esta grave carencia intenta salvarla el propio Consejo, artífice de tamaño desatino, señalando como "la obligación impuesta a los Estados miembros de garantizar a toda persona *el derecho a conocer la existencia de un tratamiento*, previsto en el antiguo artículo 10 de la propuesta modificada, se ha recogido en el artículo 21 en forma de obligación de garantizar la publicidad de los tratamientos" [38].

Establecido por tanto, no como derecho del afectado, sino como obligación inherente al responsable del tratamiento, su articulación presenta un régimen dual:

1. Información al interesado durante la recogida de datos.

El *art. 10* garantiza a las personas de las que se recaban datos personales el derecho a determinada información específica.

La recogida leal y legítima de datos personales presupone que el interesado decida divulgar o no los datos que le conciernen, basándose en un conocimiento fiable de la finalidad del tratamiento, el carácter obligatorio o facultativo de la obligación de divulgar los datos en cuestión y todas las consecuencias que podrían derivarse de una ausencia de respuesta. Para que pueda ejercer sus derechos y controlar con eficacia la utilización de los datos que le conciernen, debe asimismo estar informado acerca de los destinatarios de los datos, así como de la existencia de sus derechos de acceso y rectificación de los datos que le conciernen.

Entre las menciones introducidas en este artículo, merece reiterarse claramente que cuando los datos se recaban de los interesados, el hecho de obtener la información no es sólo un derecho del interesado, sino una obligación del responsable del tratamiento.

2. Información cuando los datos no han sido recabados del propio interesado.

Con objeto de permitir al interesado el ejercicio de sus derechos exige el *art. 11* del responsable del tratamiento que garantice que se informe al interesado de la comunicación de los datos que le conciernen. El interesado puede de este modo ejercer su derecho de acceso y oponerse a que se continúe realizando el tratamiento en cuestión.

Además de la finalidad del tratamiento, de las categorías de datos tratados y del nombre y dirección del responsable del tratamiento, se ha considerado necesario, como no podía ser de otro modo, informar también al interesado sobre los

[38] Ibídem.

destinatarios o categorías de destinatarios y la existencia de su derecho de acceso, rectificación y oposición.

Tal información deberá producirse en el momento del registro de los datos, o en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos.

Respecto a las *exenciones* a la obligación de informar al interesado destacar nuevamente la que opera con respecto a los tratamientos con fines estadísticos o de investigación histórica o científica.

Asimismo se incluyen unos peculiares supuestos excepcionadores: cuando dicha información resultara imposible, o exigiera esfuerzos desproporcionados. La imposibilidad debe entenderse como la inexistencia de cauces de comunicación con el afectado, tales como su ausencia, cambio no notificado de domicilio, etc.

Más complejo resulta la determinación de que sea "esfuerzos desproporcionados". ¿ Esfuerzos económicos o esfuerzos en la localización del afectado ? Supuesto ciertamente indeterminado y de difusos contornos.

Se establece además que, ante tales situaciones, los Estados miembros deben prever las garantías apropiadas. Obviamente para velar por que la falta de información no suponga menoscabo de los derechos y libertades del interesado.

b) Derechos de Acceso, Rectificación y Cancelación.

Recogidos en su *art. 12*, se articulan en la Directiva en torno al derecho del interesado a acceder a sus propios datos personales y los derechos "complementarios" a obtener la rectificación, supresión o bloqueo de dichos datos.

Obviamente, sin la garantía del derecho de acceso, carecería de sentido toda la regulación, por cuanto considerado, junto al derecho de información, como manifestación fundamental del *"derecho a la libertad informática"*, sirve como instrumento fundamental para la correcta articulación y defensa de la "identidad" de los ciudadanos, frente a un abuso o un uso incorrecto de sus datos personales.

Se confiere al interesado el derecho a obtener, sin restricciones, con una frecuencia razonable y sin gastos ni esperas excesivos, la confirmación de la existencia o inexistencia de datos personales que le conciernen y, en caso afirmativo, la comunicación de estos datos en forma inteligible.

Además el derecho de acceso deberá, como señaló el Parlamento Europeo, poder ejercerse sin ningún tipo de coacción por parte de terceros [39].

[39] Como señaló en su Enmienda número 132.

De igual forma, en el caso de decisiones tomadas por un sistema automatizado y que dé resultados contrarios a los intereses del afectado se reconoce el derecho de éste a conocer los razonamientos utilizados en los tratamientos en cuestión.

Es a los Estados miembros a quienes incumbe precisar cómo deben ofrecerse estas informaciones al interesado. Incumbe asimismo a éstos determinar en su legislación la expresión "frecuencia razonable". Teniendo presentes los intereses y los medios del interesado y los del responsable del tratamiento, los legisladores de los Estados miembros deben prever que el responsable del tratamiento no pueda exigirle al interesado que ejerce su derecho de acceso una remuneración superior al coste real.

El derecho de acceso puede ejercerse sin restricciones. El interesado tiene derecho a obtener información sobre el origen (pero no el origen en general, lo que resultaría demasiado vago y, por consiguiente, inútil) y sobre la utilización en general (y no la utilización puntual, lo que podría resultar demasiado pesado y burocrático) de los datos personales en cuestión.

Como ya se indicó, y en consonancia con el reconocimiento del derecho de acceso, se concede a los interesados el derecho de obtener, en cada caso, la rectificación, supresión o bloqueo de los datos, cuando su tratamiento sea incompatible con la Directiva

La formula utilizada en la Directiva, "en su caso", deja a la legislación de cada Estado miembro en materia de protección de datos la tarea de adaptar los derechos del interesado sobre supresión, bloqueo o rectificación a las diferentes situaciones en las que se tratan y explotan datos personales incumpliendo esta Directiva.

Se cierra la regulación acerca de estos derechos preveyendo que los terceros a quienes se hayan transmitido datos tratados de manera incorrecta o ilegítima reciban una notificación de la rectificación, supresión o bloqueo de los datos, con objeto de que puedan rectificar, suprimir o bloquear a su vez los datos en cuestión.

c) Derecho de oposición del interesado.

El interesado, indica el *art. 14*, tiene derecho a oponerse en cualquier momento y por motivos legítimos personales, a que los datos personales que le conciernan sean objeto de tratamiento. Los motivos legítimos pueden ser la falta de justificación legal de un tratamiento determinado de datos personales.

Este derecho deberá reconocerse en todo caso en los supuestos recogidos en los puntos e) y f) del art. 7. Es decir, aquellos tratamientos necesarios para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuni-

quen los datos; así como aquellos tratamientos necesarios 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.

En caso de oposición ejercida en las condiciones previstas anteriormente, el responsable del tratamiento debe suspender el tratamiento referido a dichos datos.

Por otro lado, como ha señalado el Parlamento Europeo, el derecho de oposición debe poder ejercitarse en cualquier momento y, en particular, frente a los tratamientos con fines de prospección [40].

Estas obligaciones deben aplicarse independientemente del carácter de la prospección; de que se trate de una prospección comercial o de que la efectúe un organismo de caridad o un partido político. Estas obligaciones, consagración de los denominados "ficheros Robinson" [41], se concretan en dos específicas manifestaciones:

1. Derecho de oponerse, previamente y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección.

2. En caso de comunicación de datos a terceros o de utilización en nombre de éstos a efectos de prospección, derecho a ser informado antes de los que los datos se comuniquen por primera vez o sean utilizados. Igualmente, supone el reconocimiento del derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Estas previsiones se refieren exclusivamente a la prospección por escrito. Las medidas encaminadas a proteger a las personas contra solicitudes no deseadas y realizadas por medios de telecomunicación se tratan en la propuesta modificada de Directiva relativa a la protección de las personas en el ámbito de las redes de telecomunicación [42].

Se impone a los Estados miembros la obligación de adoptar todas las medidas necesarias para que los ciudadanos conozcan el derecho que les asiste a oponerse al tratamiento de sus datos personales con fines de prospección.

[40] Recoge las Enmiendas núms. 30 y 145 del Parlamento Europeo.

[41] Cfr. PEREZ LUÑO, A.E., "Comentario Legislativo: La LORTAD y los derechos fundamentales", en Derechos y Libertades. Revista del Instituto Bartolomé de las Casas, 1993, febrero-octubre, nº 1, pp. 405-424; Derechos Humanos, Estado de Derecho y Constitución, 5ª edic., Tecnos, Madrid, 1995, pp. 416-419.

[42] Cfr. Propuesta modificada de Directiva del Parlamento Europeo y del Consejo, relativa a la protección de los datos personales y la intimidad en relación con las redes digitales de telecomunicación y, en particular, la Red Digital de Servicios Integrados (RDSI) y las redes móviles digitales públicas, COM (94) 128 final/2-COD 288, Bruselas, 15.06.1994.

d) Derecho a no verse sometido a decisiones individuales automatizadas perjudiciales.

El *art. 15* de la Directiva establece el derecho de las personas a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, y que tenga como único referente un tratamiento automatizado de datos personales tendente a la evaluación de determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc. Tres elementos deben, de esta forma, concurrir para que tal derecho sea efectivamente desplegado:

1. Debe tratarse de un decisión basada exclusivamente en un tratamiento automatizado. Se excluyen, por tanto, aquellas decisiones que, aún teniendo como eje central un tratamiento de tal naturaleza, cuenten con otros elementos o criterios que coadyuven a su adopción.

2. El tratamiento automatizado debe ir referido a la consideración de determinadas actitudes, comportamientos o tendencias de las personas afectadas. Aquí radica precisamente el peligro que incorporan tales decisiones individuales automatizadas, por cuanto la consideración global de una persona se hace exclusivamente sobre la base de una concreta manifestación de su personalidad o conducta.

3. La decisión adoptada debe incorporar efectos jurídicos o afectar de manera significativa a los afectados. Obviamente, debemos pensar en decisiones que sean perjudiciales, y que incorporen alguna clase de perjuicio, bien sea material, bien moral.

Con arreglo al apartado 2, la persona puede verse sometida a una decisión similar a las contempladas en el apartado 1 cuando ésta se haya tomado a raíz de un contrato concluido entre ella y el responsable del tratamiento, siempre que la persona obtenga satisfacción o que unas medidas apropiadas, como la posibilidad de defender su punto de vista, garanticen la salvaguarda de sus intereses legítimos. Esta garantía puede emanar de la ley, de los procedimientos de notificación o incluso de medidas de tipo interno que hubiera adoptado la empresa.

Ahora bien, el dejar a las empresas el establecimiento de las "medidas apropiadas" resulta un medio escasamente eficaz para la defensa de los derechos de los ciudadanos, de sus intereses legítimos.

Tales garantías, por su importancia, deberían emanar de las propias normas reguladoras de estos supuestos, pues de lo contrario el principio de seguridad jurídica se vería gravemente conculcado. Además la diferente organización y gestión empresarial, sus diferentes ámbitos de concurrencia y su distinta implantación, hacen imposible la adopción de unas medidas homogéneas aplicables a este supuesto.

Como remate a este punto, señalar que la Directiva también permite que una persona pueda verse sometida a una decisión individual automatizada, cuando así lo autorice una ley; y siempre que la misma prevea las medidas adecuadas que garanticen el interés legítimo del interesado.

2.6. *Categorías especiales de tratamientos: La regulación de los Datos Sensibles.*

Se suele admitir que los derechos de los ciudadanos están amenazados no por el contenido de los datos personales, sino por el contexto en que se sitúa el tratamiento de dichos datos. Existe, sin embargo, un amplio consenso entre los Estados Miembros sobre el hecho de que ciertas categorías de datos, por su propia naturaleza, además de por el contexto en el que se tratan, pueden poner en peligro los derechos fundamentales de los interesados.

El *art. 8* plantea así el intento de establecer límites estrictos al tratamiento y a la explotación de las siguientes categorías de datos especiales: *origen racial o étnico* (incluida la información sobre el color de la piel); *opiniones políticas, convicciones religiosas o filosóficas,* (estas categorías engloban informaciones sobre las actividades del interesado en el terreno político, religioso o filosófico); *la pertenencia a sindicatos* [43]; así como el tratamiento de los datos relativos a *la salud del interesado* (incluidas la información sobre su estado físico o mental en el pasado, presente y futuro [44], así como sobre el abuso de drogas y de alcohol) o a *la sexualidad.*

Respecto a estos datos precitados, la regla general es la prohibición de su tratamiento [45].

Ahora bien, establecida esta prohibición general, el sistema protector se desvirtúa gravísimamente por el amplio elenco de excepciones que se contemplan. Si bien algunas parecen tener cierta razón de ser, otras, sin embargo, no suponen más que la institucionalización de un amplio marco de arbitrariedad estatal.

[43] Resulta sorprendente la diferenciación entre opiniones políticas y afiliación sindical. Para las opiniones sindicales se exige el requisito suplementario de la afiliación. El conocimiento de las opiniones políticas tiene también su principal baluarte en la afiliación de los ciudadanos a los diferentes partidos políticos. Así pues, o bien se prescinde en ambos casos del requisito de la afiliación como elemento delimitador de la adscripción a una determinada opción política; o bien se exige en ambos, limitando así el ámbito material protegido.

[44] La referencia al estado mental en el futuro nos parece especialmente grave, por cuanto supone ingresar a los afectados en una especie de "censos negros", sin posibilidad alguna de defensa al depender la confirmación de la "sospecha" de una realización practica, que no tiene actualmente ninguna constatación fáctica.

Debería seguirse en esta materia la Recomendación elaborada por el Consejo de Europa, respecto a la protección de los datos personales en el sector médico. Vid. sobre ello: Conseil de l´Europe. Recommandation Nº R (81) 1 du Comité des Ministres aux États membres relative à la réglementation applicable aux banques de données médicales automatisées (adopté par le Comité des Ministres le 23 janvier 1981, lors de la 328 reunion des Délégues des Ministres).

[45] Dicho tratamiento incluye tanto el automatizado como el no automatizado, tal y como solicitó el Parlamento en su Enmienda número 63.

do señalaba que no bastaba la concurrencia *per se* de ese interés para apreciar la concurrencia de tal excepción, sino que ese interés debía ser imperativo, y además debidamente justificado. Es decir, no bastaba con su mera alegación; debía probarse su concurrencia.

f) una función de control, de inspección o reglamentaria relacionada con el ejercicio de la autoridad pública en los casos referidos a la seguridad pública, actuaciones penales y policiales y defensa de intereses económicos y/o financieros.
g) la protección del interesado o de los derechos y libertades de otra persona. Estos intereses pueden, entre otros, comprender: los secretos de negocios de terceros; las normas del secreto profesional a que están sometidas las profesiones jurídicas o médicas; el derecho de un tercero a elaborar su propia defensa en litigios; etc.

Además, y por si aún fuera poco, se autoriza a los Estados Miembros a limitar los derechos del interesado, tal y como se establecen en el art. 12, cuando los datos vayan a ser objeto de un tratamiento con fines exclusivamente científicos o se guarden durante el tiempo necesario para la elaboración de estadísticas, ya que se considera que dichas operaciones no constituyen un riesgo importante para el interesado.

Pero si graves son las excepciones, más lo es la supresión en el texto de la Directiva de la posibilidad contenida en la Propuesta del 90. El antiguo art. 14.2 preveía, en el supuesto de que el interesado no pudiera tener acceso a datos que le concernían y que figuraran en un fichero, debido a la protección de un interés cubierto, que la Autoridad de control debía, previa solicitud, proceder a las verificaciones y a los controles necesarios del fichero en el que figuran los datos en cuestión. El objeto de este control era el de verificar la licitud de los tratamientos con relación a los criterios que planteaba la entonces Propuesta de Directiva. Al efectuar este control, la autoridad debería evitar atentar contra los intereses cuya salvaguarda contemplaba su apartado 1.

En la Directiva vigente, se ha pretendido compensar esta ausencia, como señala el Consejo, con la inclusión en al art. 28 de la posibilidad de control efectuada por la Autoridad de control a petición del interesado en caso de que se restrinja el derecho de acceso [77].

Tampoco debe olvidarse a este respecto, lo señalado por la Directiva en su *art. 9* donde se insta a los Estados miembros a que establezcan, para los organismos de prensa y del sector audiovisual, excepciones a las disposiciones de la Directiva, en la medida en que sean necesarias para conciliar los derechos fundamentales

[77] Cfr. Posición Común (CE) Nº 1/95, adoptada por el Consejo el 20 de febrero de 1995..., cit., p. 23.

del individuo, y en particular el derecho a la intimidad con la libertad de expresión, pues hay un riesgo de conflicto entre ambas categorías [78] [79].

2.14. *Disposiciones Finales.*

Se prevé en el *art. 32* una medida transitoria encaminada a permitir que las medidas adoptadas en aplicación de la Directiva y relativas a los tratamientos efectuados antes de la entrada en vigor de estas normas se declaren vigentes de manera progresiva. Parece conveniente fijar un plazo de tres años para que así sea.

El informe periódico elaborado por la Comisión, tal y como señala el *art. 33*, sobre la aplicación de la Directiva, que será presentado al Consejo y al Parlamento, será publicado [80]. Para tener en cuenta los desarrollos tecnológicos, sobre todo en el marco de la evolución de la sociedad de la información, la Comisión estudiará en particular en su informe periódico la aplicación de la Directiva a los tratamientos de carácter personal en forma de sonidos e imágenes.

B. LA PROTECCION DE LOS DATOS PERSONALES EN LA EUROPA DE SCHENGEN.

1. LOS ACUERDOS DE SCHENGEN.

La firma del *Acuerdo de Schengen* entre los gobiernos de los Estados del Benelux (Luxemburgo, Países Bajos y Bélgica), de la Republica Federal de Alemania y de la República Francesa tuvo lugar el 14 de junio de 1985 en la localidad fronteriza luxemburguesa que da nombre al Acuerdo [81] [82].

[78] Acerca de la consideración de estos derechos en la legislación, jurisprudencia y doctrina española, vid., entre otros: BUSTOS PUECHE, J.E., "Los límites de los derechos de libre expresión e información según la jurisprudencia", en la obra colectiva, edic. a cargo de L. García San Miguel, Estudios sobre el derecho a la intimidad, Tecnos & Universidad Alcalá de Henares, Madrid, 1992, pp. 101-156; ESPINAR VICENTE, J.M., "La primacía del derecho a la información sobre la intimidad y el honor", ibid., pp. 46-67.

[79] La no delimitación comunitaria de los ámbitos de intimidad personal y libertad de expresión supone conceder, de facto, a los periodistas una auténtica "patente de corso" para el desarrollo de sus actividades.

[80] Recoge la Enmienda número 95 del Parlamento Europeo.

[81] Cfr. LAZARO MORENO, F., El Acuerdo de Schengen y la libre circulación de personas en la CEE, Cuadernos de Europa, nº 2, Diputación de Zaragoza (Comisión de Europa), Zaragoza, 1993.

[82] Como antecedentes de este Acuerdo pueden citarse, tal y como se desprende de los propios datos explicitados en su texto, los siguientes hechos:

- Conclusiones de la Reunión de Neustadtñaisch, de 31 de mayo de 1984, de los Ministros de Transportes de los Estados del Benelux y la República Federal de Alemania.
- Declaración del Consejo Europeo de Fontainebleau, de los días 25 y 26 de junio de 1984, relativa a la supresión en las fronteras interiores de las formalidades de policía y de aduanas para la circulación de personas y mercancías.

Este acuerdo de 1985 hacía referencia en numerosos preceptos a una convención ulterior, destinada a completarlo y precisar su contenido. Este fue el objeto del *Convenio de Aplicación del Acuerdo de Schengen*, firmado el 19 de junio de 1990 [83], y que ha entrado en vigor el 26 de marzo de 1995 para siete de los países firmantes (Alemania, Belgica, España, Francia, Holanda, Luxemburgo y Portugal); no sin ciertos problemas y constantes tensiones [84].

El Convenio de Aplicación de Schengen responde a la finalidad de suprimir los controles en las fronteras interiores y toma como punto de referencia la existencia de un *"espacio interior común"* [85].

Pero, la sustitución de los controles internos, además de medidas de armonización legislativa y de mejora de la asistencia judicial internacional en materia penal, hace necesario un mejor intercambio en la información [86].

[83] Italia se adhirió al Acuerdo de 1985 el 27 de noviembre de 1990; España y Portugal el 25 de junio de 1991; Grecia el 6 de noviembre de 1992. Los cuatro países se han simultáneamente adherido a la Convención de aplicación.

Tras la ampliación de la Unión, el 1 de enero de 1995, uno de los tres nuevos socios, Austria, ha firmado los instrumentos de adhesión a Schengen el 28 de abril de 1995. Finlandia, Dinamarca y Suecia se adhirieron el 19 de diciembre de 1996; al igual que otras dos naciones asociadas no miembros de la Unión Europea: Islandia y Noruega.

Respecto a los otros Estados Miembros se mantienen, hasta el momento, al margen Gran Bretaña e Irlanda en razón - al menos eso argumentan sus respectivos gobiernos - de la ausencia de fronteras comunes con el resto de Estados Miembros.

Cfr. GARCIA GALAN, J.L., "La libre circulación de personas en el Espacio Schengen, una realidad desde 1995", en Rev. Europa Junta, núm. 37, abril 1995, p. 15.

[84] El oscurantismo con el que se trabaja en este ámbito por parte de los Estados firmantes, y sus constantes cambios de opinión respeto a la aplicación efectiva del Convenio, impide conocer con exactitud su grado real de cumplimiento.

Así Francia recientemente ha aplicado la cláusula de salvaguardia, como medio de defensa frente a los atentados terroristas de grupos islámicos que están teniendo lugar en su territorio. Este mismo país ha tenido también enfrentamientos con Holanda, debido a lo permisivo de la legislación neerlandesa respecto a la tenencia y consumo de determinadas sustancias estupefacientes. En España y Portugal ya han surgido problemas con nacionales de países latinoamericanas o de las antiguas colonias, que han creado un cierto clima de rechazo social a estas medidas. Mi agradecimiento al Prof. Andres Rodriguez Benot por ponerme al tanto de estas circunstancias.

[85] Cfr. DE LUCAS, J., El desafío de las fronteras, Temas de Hoy, Madrid, 1994. Asimismo, ESCOBAR HERNANDEZ, C., "El Convenio de aplicación del Acuerdo de Schengen y el Convenio de Dublín: Una aproximación al asilo desde la perspectiva comunitaria", en Revista de Instituciones Europeas, Vol. 20, núm. 1, 1993, pp. 69-70.

[86] Cfr. DE MIGUEL ZARAGOZA, J. y BLANCO DE CASTRO, A., "El Título VI del Tratado de la Unión Europea: Cooperación en asuntos...", cit., pp. 212-213.

Con objeto de conseguir ese mejor intercambio de información se introduce una de las principales innovaciones de este convenio: un complejo sistema informático, denominado *Sistema de Información de Schengen*, constitutivo del soporte para la transmisión automatizada de los datos necesarios para la consecución de los precitados objetivos [87].

2. EL SISTEMA DE INFORMACION SCHENGEN (S.I.S.)

2.1 *Naturaleza y Funciones.*

Este fichero, "contrapunto necesario a la supresión de los controles en las fronteras", constituyó el tema central de los debates del acta adicional.

Considerado como un gran riesgo de atentado a las libertades individuales, almacenará globalmente 800.000 señalamientos de personas buscadas y 6.000.000 de objetos [88].

Regulado en el *TITULO IV* del Convenio de Aplicación, este Sistema permitirá, mediante un procedimiento de consulta automatizado, que las Autoridades designadas por las Partes Contratantes [89], dispongan de descripciones de personas y de

[87] Para un estudio más detallado sobre los Acuerdos de Schengen, vid.: SANCHEZ BRAVO, A., "La protección de los datos personales en la Europa de Schengen", en Actas del II Congreso Internacional de Informática y Derecho (Volumen II), en Informática y Derecho, Vol. 12-13-14-15, 1996, pp. 1401-1459.

[88] Cfr. NEEL, B., "L´Europe sans frontières intérieures: l´Accord de Schengen", en Actualité juridique. Droit Administratif, 1991, núm. 10, p. 664.

[89] Respecto a la determinación de las autoridades competentes, conviene remitirse a lo establecido en el art. 101 donde se establece la enumeración de aquéllas a las que se reconoce los "derechos" de acceso y consulta a los datos integrados en el Sistema de Información de Schengen.

Dicho artículo señala: "El acceso a los datos...., así como el derecho de consultarlos directamente estará reservado exclusivamente a las autoridades competentes para:

a. los controles fronterizos
b. las demás comprobaciones de policía y de aduanas realizadas dentro del país, así como la coordinación de las mismas.".

Asimismo se reconocen tales facultades, acceso y consulta, "a las autoridades competentes para la expedición de visados, ... autoridades centrales competentes para el examen de las solicitudes de visado y por las autoridades competentes para la expedición de permisos de residencia y para la administración de extranjeros...".

Será Cada Parte Contratante la que facilitará al Comité Ejecutivo la lista de las referidas "autoridades competentes".

Al respecto cabe hacer dos breves consideraciones:

1. La determinación de dichas autoridades se hace de manera genérica, en consideración a la tarea a desarrollar. Esta generalidad supone un evidente riesgo de ampliación cuantitativa de aquellas personas o entidades que tendrán acceso a los datos, con el evidente riesgo de peligro para los derechos de los ciudadanos. Máxime cuando no se establece ningún control para tal determinación.

2. Resulta sorprendente la exclusión de las autoridades judiciales de la enumeración señalada. Parece que sólo las autoridades policiales y administrativas poseen tales facultades. Este "olvido" supone un manifestación de la consolidación de esta "Europa policial", que parece va perfilándose.

objetos, en el territorio de cada uno de los Estados [90]. Dichas descripciones sólo figurarán siempre y cuando las mismas afecten a todas las Partes Contratantes. Este criterio "restrictivo", digno de ser indicado, impedirá que mal entendidas necesidades o intereses particulares de alguno/os Estado/s Miembro/s ponga en peligro la función y el funcionamiento uniforme y unificado del sistema.

2.2. *Categorías de Datos. Problemática.*

La categoría de los datos que se incluirán en el Sistema de Información de Schengen se establece de acuerdo a dos criterios:

a. Categorías de datos aportados por cada una de las Partes Contratantes (*ratione personae*).
b. Dichos datos deben ser necesarios para los fines señalados en los artículos 95 a 100 (*ratione materiae*) [91].

Respecto a la necesidad de la introducción de los datos en el Sistema, será cada Parte Contratante la que determinará si la importancia del caso justifica la introducción de la descripción. Se deja por tanto a cada Estado la facultad absoluta de proceder a esa ponderación. Ello es coherente con el carácter proteccionista para los intereses de los Estados que consagra el Convenio, así como con las facultades que los Estados mantienen en orden a la determinación de su política de seguridad y de orden público. Lo que no se acierta a comprender es como se conseguirá alcanzar esa "unidad" que el Convenio pretende, si se mantienen esos amplios márgenes de autonomía.

Además como indicamos anteriormente sólo se introducirán aquellas descripciones que afecten a todas las Partes Contratantes, por lo cual deberá procederse a una clara delimitación de cuando nos encontramos ante esa "afección común".

Para arrojar más incertidumbre en esa alternativa - intereses nacionales vs. consecución objetivos comunes -, el propio Convenio concede la facultad a cualquiera de las Partes Contratantes de añadir posteriormente a la introducción de una descripción una indicación destinada a que la ejecución de la medida pertinente no se realice en su territorio [92].

[90] Cfr. NEEL, B., "L´ Europe sans frontières intérieures: l´Accord de Schengen", cit., p. 665.

[91] Artículo 94.

[92] Art. 93.4. Dicha indicación se introducirá cuando se estima que la referida inscripción no es compatible con el Derecho nacional, obligaciones internacionales o intereses nacionales esenciales de la Parte Contratante.

El Propio Convenio manifiesta así la falta de coordinación que existe entre los Estados Miembros en orden a la aproximación y unificación tanto de sus políticas en materia de seguridad, como en sus "productos legislativos".

Tal indicación restrictiva sólo podrá llevarse a efecto cuando la identificación se haya realizado de conformidad con los artículos 95, 97 ó 99. A saber: Personas buscadas para su detención a efectos de extradición; personas desaparecidas o personas que, en interés de su propia protección o para la prevención de amenazas, deban ser puestas a salvo provisionalmente; personas o vehículos a efectos de vigilancia discreta o control específico.

La categoría de los datos que se introducirán en el S.I.S. aparecen indicados en el *párrafo 2 del artículo 94*, si bien su desarrollo pormenorizado se efectúa en los artículos siguientes (*arts. 95-100*).

Dichas categorías de datos son:

a. personas descritas.
b. objetos y vehículos.

Con referencia a las personas, el Convenio permite la introducción de todo un elenco de datos personales, en una enumeración excesivamente prolija, y que en algunos supuestos pueden presentar evidentes problemas para los derechos de los individuos afectados. Dichos datos son: nombre y apellidos; alias en su caso, que se registrarán por separado; rasgos físicos particulares, objetivos e inalterables; primera letra del segundo nombre; fecha y lugar de nacimiento; sexo; nacionalidad; indicación de que el interesado va armado o es violento; el motivo de la inscripción; y la conducta a observar.

No obstante, no podrán registrarse sin limitación alguna datos sobre los interesados. El límite se encuentra en los denominados " datos sensibles", a los que el propio Convenio hace referencia por remisión al art. 6 del Convenio 108 del Consejo de Europa para la protección de las personas en lo referente al tratamiento automatizado de los datos de carácter personal [93].

[93] El art. 6 del Convenio 108 del Consejo de Europa establece: "Los datos de carácter personal que revelaren el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán ser elaborados automáticamente a menos que el Derecho interno previere las oportunas garantías. La misma regla se aplicará a los datos de carácter personal referentes a condenas criminales".

Establece así el Convenio la prohibición del tratamiento automatizado de esta clase de datos, en función de las potencialidades lesivas que presentan para los derechos e intereses de los individuos. Discrepamos en este punto de la opinión manifestada por Manuel Heredero ("La protección de datos personales en manos de la policía: reflexiones sobre el Convenio de Schengen", en la obra colectiva La protección de los datos personales. Regulación internacional de la seguridad informática, Monografies i Documents, 8, Centre d´Investigació de la Comunicació i Universitat Pompeu Fabra, Generalitat de Catalunya, Barcelona, 1993, p. 38) en orden a que el Convenio 108 no prohíbe el tratamiento de estas clase datos, sino que lo condiciona a la adopción en el Derecho interno de unas garantías apropiadas. Estimanos que lo que el precitado Convenio establece es la prohibición de dicho tratamiento con carácter general, permitiendo algunas excepciones a esta regla en virtud de la naturaleza protectora de las medidas que se arbitren en el Derecho interno. Lo general, por lo tanto, es la prohibición, y no la excepción.

Como señala el propio Consejo de Europa la lista que contiene el artículo 6 no deberá considerarse exhaustiva. El grado de sensibilidad de los datos dependerá del contexto jurídico y sociológico del respectivo país.

En España la LORTAD establece también en su art. 7, una protección reforzada para este tipo de datos, que enumera bajo la denominación genérica de "datos especialmente protegidos".

El registro de las condenas criminales anteriores no se incluye, puesto que no figuran en la proposición primera del art. 6 del Convenio 108 y además condicionan algunas de las situaciones de las personas buscadas (en especial el supuesto contemplado en el *art. 96*) [94].

Conviene detenerse brevemente en uno de los supuestos recogidos en la enumeración que acabamos de indicar. Se trata de "*los rasgos físicos particulares, objetivos e inalterables*". La no determinación de que deba entenderse por tales rasgos constituye un supuesto de evidente indefinición e inseguridad. La inclusión dentro de tal concepto de datos como el color de la piel o el origen étnico, podría dar lugar a una peligrosa antinomia, al vulnerar la prohibición establecida en el propio Convenio en orden a la no inclusión en el Sistema Informático de datos sensibles.

Estimamos, que lo que se establece es la posibilidad de introducir datos pertenecientes a la referida categoría, siempre y cuando aquéllos no tengan la naturaleza de sensibles. Sería una determinación residual por exclusión, en la cual entrarían supuestos tales como cicatrices, minusvalías físicas, etc... Obviamente, otras interpretaciones pueden darse a esta problemática, nosotros indicamos la que estimamos más acorde a lo que parece derivarse del propio precepto y del conjunto del Convenio.

Las categorías de datos son ampliamente reguladas en los artículos 95 a 100, de acuerdo a los diferentes datos que son necesarios o se derivan del cumplimiento de los fines que se establecen en el Convenio. Pasemos a analizarlas.

2.2.1. Datos relativos a personas buscadas para su detención a efectos de extradición [95].

Su introducción en el Sistema sólo se realizará cuando medie un requerimiento de la autoridad judicial competente para conocer de tal procedimiento.

Se conculca de esta manera la autonomía de las referidas autoridades judiciales en orden a la ordenación del procedimiento, por cuanto su requerimiento no surte un efecto automático, sino que se difiere a la "aprobación" de otras e indefinidas autoridades nacionales (por no decir policiales).

Podría parecer, que estas medidas constituyen una salvaguarda para la protección de los datos personales que se solicitan. Nada más lejos de la realidad. Si el Poder Judicial tiene encomendado en los Estados de Derecho la salvaguarda de los

[94] Cfr. HEREDERO HIGUERAS, M., "La protección de datos personales en manos de la policía: reflexiones sobre el Convenio de Schengen", en la obra colectiva La Protección de los datos personales. Regulación Internacional de la seguridad informática, Monografies i Documents, núm. 8, Centre d'Investigació y de la Comunicació i Universitat Pompeu Fabra, Generalitat de Catalunya, Barcelona, 1993.

[95] Art. 95.

derechos e intereses de los ciudadanos, no se acierta a comprender como se le desposee de tales facultades, y se sustituye por un control de oportunidad o interés nacional, que responden a intereses ciertamente políticos y no jurídicos.

Junto a los datos personales que se integrarán en la descripción, el precepto establece que deberá aportarse una serie de información suplementaria, calificada como "esencial ", y que deberá ser simultánea a la descripción. Estas menciones formales, o más concretamente procedimentales son: autoridad que pide la detención; existencia de una orden de detención o de un documento que tenga la misma fuerza, o de una sentencia ejecutoria; carácter y calificación legal de la infracción; descripción de las circunstancias en que se cometió la infracción, incluidos el momento, el lugar y el grado de participación de la persona mencionada; en la medida de lo posible, las consecuencias de la infracción.

Nada se dice acerca de las garantías que deben incorporarse a esta transmisión de carácter técnico, que revestirá casi con toda probabilidad la forma de transmisión automática informatizada, y que además el propio Convenio exceptúa de las garantías referentes a la protección de los datos personales, según se desprende de lo señalado en los arts. 126 y 127.

No olvidemos que las referidas " menciones formales", incorporarán una serie de datos personales, que por esta vía escaparán a las ya de por sí escasas garantías que presenta el Convenio [96].

2.2.2. Datos relativos a extranjeros que estén incluidos en la lista de no admisibles [97]

La introducción de los referidos datos se hará sobre la base de una descripción, que deberá atemperarse a los procedimientos legalmente establecidos para la adopción de las correspondientes decisiones de no admisión en el territorio nacional [98].

En este supuesto, a diferencia del anterior, si parecen tener un efecto directo las decisiones adoptadas, cuya sola concurrencia posibilita la introducción de la descripción en el Sistema. Ahora bien, en este supuesto, no sólo serán las decisiones adoptadas por las autoridades judiciales, sino también las realizadas por las autoridades administrativas; entiéndase por tales las que tienen encomendadas el control y la administración de extranjeros.

[96] Sobre esta materia, vid. Convenio Europeo de Extradición, de 13 de diciembre de 1957, así como su Protocolo Adicional de 15 de octubre de 1975 y su Segundo Protocolo Adicional de 17 de marzo de 1978.

[97] Art. 96.

[98] No obstante el art. 25 del Convenio de Aplicación establece la posibilidad de expedir, por una Parte Contratante, un permiso de residencia a un extranjero incluido en la lista de no admisible. Tal expedición sólo podrá tener lugar, como indica el precepto, por "motivos serios", especialmente de carácter humanitario o derivados de obligaciones internacionales. Esta expedición conllevará la retirada de la descripción del S.I.S.

Esta excepción implica una manifestación más de la falta de unidad entre los Estados Miembros, y la descoordinación que ello conllevará en el otorgamiento de los permisos de residencia. La salvaguarda de la "autonomía" de los Estados se manifiesta como principal obstáculo para la consecución de una política común en este ámbito.

La determinación de esta categoría de personas suscita evidentes inquietudes[99]. Los extranjeros señalados a efectos de no admisión, que son objeto de una negativa de entrada sobre el territorio de uno de los nueve Estados, pueden serlo porque tal decisión esté basada en la falta de presentación de uno de los documentos exigidos por la legislación nacional. Dicha prohibición se aplicará al conjunto del territorio común.

Esta decisión, como señala el prof. Julien-Laferriere, aparte de suponer un atentado a la soberanía de los Estados, que son tributarios de decisiones adoptadas por autoridades extranjeras, revela una desproporción evidente entre el hecho imputable al extranjero y las consecuencias que se derivan de él [100].

Dos son las razones que pueden justificar una decisión tal:

a. Amenaza para el orden público o la seguridad nacional, si bien aquí matizados por el peligro que pueda suponer la presencia de un extranjero sobre el territorio nacional.

El artículo establece dos supuestos o categorías concretas, como señeras de lo que debe entenderse por tal "amenaza":

1. Extranjero condenado por una infracción sancionada con pena privativa de libertad de un año como mínimo.

La discrecionalidad del supuesto, y su vulneración de los postulados de la seguridad jurídica, es evidente. Lo determinante es que la pena sea privativa de libertad, obviando otra serie de sanciones penales que, pese a que no incorporan tal privación, pueden considerarse también como graves y que merecen el reproche social. Pero quizás lo más polémico será el hecho de la aplicación extraterritorial de los efectos o consecuencias de una determinada ley penal nacional. La existencia en los diversos Estados Miembros de legislaciones penales diferentes, con tipificaciones legales, procedimientos y órganos jurisdiccionales diversos, complica aún más el esclarecimiento de este supuesto.

[99] Especialmente sensible se ha mostrado sobre estas cuestiones el Prof. Javier de Lucas. Así, y de entre su numerosa producción científica, vid.: Europa: ¿Convivir con la diferencia?, Tecnos & Fundación Enrique Luño Peña, Madrid, 1992; El concepto de solidaridad, Fontamara, México, 1993; El desafío de las fronteras, Ediciones Temas de Hoy, Madrid, 1994.

[100] Cfr. JULIEN-LAFERRIERE, F., "L'Europe de Schengen: de la disparition des frontières aux transferts des contrôles (commentaire de la loi nº 91 - 737 du 30 juillet 1991 autorisant l' adhésion de la France à la Convention d´application de l' accord de Schengen)", en Actualité Législative Dalloz, nº 13, 1993, p. 129.

Pensemos en una infracción tipificada como delictiva en un Estado Miembro y sancionada de acuerdo a su peculiar procedimiento, pero que sin embargo no constituye tal categoría, de acuerdo a la legislación penal de otra Parte. Surge entonces la pregunta: ¿Podrá considerarse vinculado un Estado soberano, por decisiones adoptadas por otros Estados, también soberanos, y verse compelido a la adopción de determinadas acciones, que ni siquiera puede fiscalizar?. La respuesta práctica es la cierta vinculación, que llevará a que el extranjero incluido en tal "lista" no puede acceder al conjunto del territorio del "espacio Schengen". Nuevamente se revela la necesidad de proceder a una armonización de las legislaciones penales y administrativas de los Estados Miembros, que tanta incidencia tienen sobre los ciudadanos. La generalización que parece derivarse del Convenio es ciertamente peligrosa [101].

2. Extranjero sobre el cual existan razones serias para creer que ha cometido hechos delictivos graves, o sobre el cual existan indicios reales de que piensa cometer tales hechos en el territorio de una Parte Contratante.

Nuevamente se vuelve a echar mano de conceptos jurídicos indeterminados, de estricta valoración subjetiva, y que por ello son difícilmente fiscalizables por las autoridades encargadas de su aplicación. Ello constituye un evidente peligro de vulneración de las garantías establecidas para las personas en los Estados sociales y democráticos de Derecho.

Será por lo tanto preceptivo analizar la situación caso por caso, teniendo en cuenta las circunstancias particulares que concurran en un supuesto, para no establecer una generalización sancionatoria, por el simple hecho de proceder de determinados países, étnias o grupos sociales.

Parece desprenderse del texto que serán las autoridades policiales las que procederán a esa determinación y, obviamente, lo harán de acuerdo a sus propios medios de investigación. Medios de investigación de naturaleza ciertamente represiva, en su consideración de lucha contra la delincuencia, pero que necesitará de un adecuado control, para evitar extralimitaciones amparándose en la salvaguarda de una mal entendida preservación del orden o la seguridad nacional.

b. Extranjero que ha sido objeto de una medida previa de alejamiento, devolución o expulsión.

Se trata de la vulneración de las legislaciones nacionales en materia de entrada y/o residencia de extranjeros.

[101] Respecto a la necesidad de unificación del Derecho Penal Europeo, vid. RUIZ VADILLO, E., "¿Que puede esperarse razonablemente de un Derecho Penal Europeo Comunitario? (Consideraciones Generales)", en Actualidad Penal, nº 34, 1993, pp. 507-530. Mi agradecimiento a D. Juan José Medina Ariza, por la sugerencia y búsqueda de esta obra. Asimismo, DIEZ SANCHEZ, J.J., El Derecho Penal Internacional (Ambito espacial de la ley penal), Colex, Madrid, 1990.

2.2.3. Personas desaparecidas o personas que, en interés de su propia protección o para la prevención de amenazas, deban ser puestas a salvo provisionalmente [102].

Este precepto se introduce como medio para preservar la vida e integridad de las personas. Parece estar pensándose en la actividad de grupos terroristas u organizaciones criminales, cuya forma de actuación incluye fundamentalmente la amenaza, la extorsión, el chantaje; cuando no, y desgraciadamente, el asesinato.

La introducción de los datos tiene en este supuesto un carácter preventivo, de salvaguarda. El fin es posibilitar que las autoridades policiales comuniquen el lugar de residencia de dichas personas y ponerlas así a salvo. Cuando dichas personas se encuentren en tránsito, el objetivo consistirá en impedirles la prosecución del viaje, y evitar que se consume un hecho atentatorio.

La coordinación de la policía, así como la rápida transmisión de la información, se revela fundamental en esta tarea.

Se hace un especial hincapié en la necesidad de protección de los menores y de aquellas personas que deban ser internadas por resolución de una autoridad competente. Se trata de sectores cuyo riesgo de desprotección y desvalimiento aumenta considerablemente en función de sus peculiares circunstancias. Puede constituir éste un buen procedimiento para luchar contra una situación habitual en nuestros días: la desaparición de menores.

2.2.4. Testigos, personas citadas para comparecer ante las autoridades judiciales en el marco de un procedimiento penal para responder sobre hechos por los cuales hayan sido objeto de diligencias, o personas a las que se deba notificar una sentencia represiva o un requerimiento para que se presente a fin de ser sometido a una pena privativa de libertad [103].

Esta larga enumeración recoge ciertos supuestos que pueden surgir en el marco de la cooperación y asistencia judicial en materia penal [104].

La descripción, que se hará a instancias de las autoridades judiciales nacionales de los Estados Miembros, tendrá por objeto facilitar el lugar de residencia o el domicilio de las precitadas personas.

[102] Art. 97
[103] Art. 98
[104] En materia de asistencia judicial penal, vid. Capítulo 2, Título III (Policía y Seguridad), arts. 48-53, del Convenio de Aplicación. Vid. también, "Convenio Europeo sobre Asistencia Judicial en Materia Penal, de 20 de abril de 1959", en Normas Españolas de Derecho Penal Internacional, Secretaría General Técnica, Centro de Publicaciones del Ministerio de Justicia, Madrid, 1989.

La inclusión de los datos referentes a personas a quienes se deba comunicar una sentencia represiva o que deban someterse a una pena privativa de libertad, parece constituir una primera fase del procedimiento general de extradición. La localización del sujeto, en un determinado territorio, permitirá solicitar a las autoridades nacionales competentes, con base en los referidos datos, su extradición para ser juzgado por los hechos que se le imputan o para cumplir la pena que previamente ha quebrantado.

2.2.5. Personas o vehículos, a efectos de vigilancia discreta o de control específico [105].

Dos son los objetivos que justifican la introducción de los referidos datos:

1. represión de infracciones penales y prevención de amenazas para la seguridad pública. Tal actividad preventiva se basa no obstante, como ya señalamos al tratar de los datos referentes a extranjeros incluidos en lista de no admisibles, en datos no siempre constatados, sino en simples presunciones atentatorias contra las libertades individuales. Se utilizan así conceptos tan indeterminados como *"indicios reales que permitan presumir"* o *"apreciación global del interesado"*. Pero lo más delicado es la posibilidad de utilización de datos personales por la única causa de que el afectado haya cometido hechos delictivos anteriores, y se suponga que va a cometer en el futuro hechos de extremada gravedad. Esto constituye un supuesto de "estigmatización", que implica un desbordamiento de los límites marcados por el principio de culpabilidad y responsabilidad penal.

2. prevención de una amenaza grave que proceda del interesado, o de otras amenazas graves para la seguridad interior y exterior del Estado. En este supuesto los riesgos se personalizan en la actuación del " interesado", si bien, y coincidiendo con el anterior, vuelve a basarse en " indicios ". Ciertamente que la actividad policial debe basarse en una serie de investigaciones previas, de averiguaciones, pero ello no debe constituir "título suficiente" para la inclusión de determinados datos personales en el S.I.S.

2.2.6. Objetos buscados con vistas a su incautación o como pruebas en un procedimiento penal [106].

Esta categoría de datos parece, en primera instancia, no incidir sobre los derechos de los ciudadanos. No obstante, si se comprobara la existencia de la descripción de un objeto encontrado se procederá a contactar con la autoridad informadora a los efectos de adoptar determinadas medidas a seguir. Y es para la adopción de estas medidas, para lo que sorprendentemente se establece la posibilidad de transmitir datos personales.

[105] Art. 99
[106] Art. 100

Si se trata de datos relativos a objetos, que se buscan a los efectos precitados, no se entiende el porqué de la inclusión de datos personales. Estos sólo podrían introducirse si se procediera a su subsunción bajo alguna de las categorías que a los mismos hacen referencia [107], y siempre que fueran estrictamente imprescindibles para la realización de las medidas a seguir. Nuevamente el Convenio vuelve a posibilitar un uso "arbitrario" de datos personales, cuya única salvaguarda reside en la referencia genérica a su adecuación "con el presente Convenio".

3. PROTECCION DE LOS DATOS PERSONALES

Estructurado el Convenio en torno a la creación y eficacia del Sistema de Información de Schengen, es necesario por lo tanto articular un sistema de garantías para los eventuales afectados por la recogida, almacenamiento, tratamiento y transmisión de los datos personales.

La existencia de estas garantías se revelan como imprescindibles para la articulación de un tratamiento automatizado de los datos que responda a las exigencias de un Estado Social y Democrático de Derecho. Es precisamente la extensión, la delimitación de estas garantías la que señalará el punto de encuentro, de equilibrio, entre las necesidades de información de los órganos y autoridades estatales y un escrupuloso respeto a los derechos y libertades de los ciudadanos.

Y es por ello que la vulneración de las mismas, no sólo supone un ataque frontal a los intereses del concreto afectado, sino que menoscaba la propia estructura democrática del sistema, convirtiendo la actuación estatal en arbitraria, y ajena a la estricta observancia de los principios de legalidad, congruencia y oportunidad de actuación.

El derecho a la intimidad, del que el ciudadano es titular, aunque sólo en una concepción teórica, se ve despojado de las garantías que le son propias, vaciándolo de contenido y quedando relegado a una mera declaración grandilocuente sin ninguna virtualidad práctica. El derecho debe ser tal, no sólo por que se tenga como titular, sino porque, llegado el caso, pueda ejercitarse.

La forma en que el Convenio aborda esta materia es ciertamente insatisfactoria. Los textos, extremadamente numerosos, consagrados a la protección de los datos adolecen de una manera manifiesta de haber sido introducidos tardiamente

[107] Ello implicaría la necesidad de una doble descripción, producida por la concurrencia de sujeto y objeto en el mismo supuesto. De otra forma debería procederse a la modificación de la descripción, por referencia al sujeto de la actuación ilegal, dejando la descripción del objeto como elemento accesorio, material, de la misma. De igual forma que el art. 107 permite la integración de descripciones referentes a personas, creemos que, mutatis mutandi, podría operarse una tal integración para este supuesto que estamos contemplando.

y aparecen dispersos a lo largo de la Convención sin otras directrices más que una serie de reiteraciones y una serie de exclusiones en cascada. Pese a ello se han alzado voces, tanto en la doctrina española como extranjera, defendiendo el acierto de tal regulación [108]. No obstante la opinión mayoritaria se muestra ciertamente crítica y preocupada. No es para menos, tal y como iremos viendo al avanzar en nuestra exposición.

3.1. *Marco Jurídico Regulador*

La protección de los datos personales aparece, como ya señalamos, dispersa a lo largo del texto. Tres momentos pueden apreciarse en dicha regulación:

a. Protección de los datos personales generados e intercambiados en el examen de una solicitud de asilo [109].
b. Protección de los datos de carácter personal y seguridad de los datos en el marco del Sistema de Información de Schengen [110].
c. Protección de los datos de carácter personal [111].

Los autores del Convenio han consagrado así una artificiosa diferenciación en la protección de los datos. No se acierta a comprender como las mismas categorías de datos, y por lo tanto, sujetas a los mismos riesgos, son tratadas de manera tan diversa, llegando incluso a excepcionarse el régimen de garantías [112]. Por su parte,

[108] Cfr. entre otros, HEREDERO HIGUERAS, M., "La protección de los datos personales en manos de la policía...", cit., p. y GAUTIER, Y., "La coopération policière: les perspectives ouvertes par le traité sur l´Union européenne du 7 février 1992", en Europe, 3 année, nº 4, Avril 1993. pp. 1-5.

[109] Art. 38 del Convenio de Aplicación.

[110] Capítulo 3 del Título IV del Convenio de Aplicación.

[111] Título VI del Convenio de Aplicación.

[112] Así se observa en el CAPITULO VI titulado "PROTECCION DE LOS DATOS DE CARACTER PERSONAL", que incorpora una derogación casi absoluta de las garantías. Excluye de su ámbito de aplicación la mayor parte de las políticas del Convenio para las cuales se revela imprescindible el tratamiento automatizado de los datos personales. Y lo efectúa en aquellos sectores que carecen de medidas protectoras en la parte del Convenio que los regula, y para los cuales parecería estar pensada la genérica protección de los datos que se articula en este Capítulo.

Así el Art. 126 establece, concretamente en su apartado 3, la necesidad de aplicación de una serie de principios de protección por lo que se refiere al tratamiento de datos personales transmitidos en aplicación del presente Convenio. Así, debe determinarse la finalidad de los datos, al igual que las personas que puedan utilizarlos; los datos deberán ser exactos, etc..

Tras proclamar estos principios, el propio artículo consagra esa excepción generalizada, esa derogación fáctica de las garantías. Y así señala: "4. El presente artículo no se aplicará a la transmisión de datos prevista en el Capítulo 7 del Título II y en el Título IV. El apartado 3 no se aplicará a la transmisión de datos prevista en los Capítulos 2, 3, 4 y 5 del Título III". Tras esta remisión se incluyen, y por lo tanto se excepcionan: Examen de las solicitudes de asilo; Sistema de Información de Schengen; Asistencia Judicial en materia penal; Aplicación del principio non bis in idem; Extradición; Transmisión de la ejecución de sentencias penales.

el derecho aplicable se manifiesta confuso, obedeciendo a una superposición [113] de órdenes normativos, algunos de los cuales no presentan ni una conexión directa, ni aún clara, con la regulación establecida en el Convenio.

La gran autonomía, por no decir casi la absoluta primacía, que se otorga a las legislaciones nacionales de las Partes Contratantes para la articulación de las medidas protectoras sobre los datos personales automatizados, evidencia la naturaleza restrictiva de la unificación [114] que se pretende llevar a efecto.

Surge de nuevo una contraposición dialéctica: Vamos a construir un proyecto común, pero vamos a hacerlo como a cada uno convenga o según nuestros propios criterios. La incongruencia es manifiesta.

Por otro lado, y como por todos es sabido, la protección de los datos personales es objeto de diferentes enfoques en los Estados Miembros; diversidad resultante, por una parte, de la carencia de legislación de algunos Estados miembros, y por otra, del diferente contenido de la legislación existente en aquellos que la poseen. En estas normas internas, aunque presentan un objeto idéntico, la protección de las personas afectadas adopta diferentes soluciones por la gran variedad de opciones posibles para asegurar tal protección. Además los progresos técnicos pueden llevar a los Estados a adoptar diferentes pautas de actuación y acentuar, si cabe aún más, las diferencias.

Como observamos, a casi nada se aplica este artículo. Queda vacío, sin ninguna eficacia práctica. Notable argucia de los autores del Convenio.

En iguales términos, y con las mismas excepciones, debemos manifestarnos respecto a los Arts. 127 (que extiende las medidas del artículo anterior a datos procedentes de ficheros no automatizados o introducidos en un fichero no automatizado. Desgraciadamente el acierto de este precepto queda obviado por las referidas excepciones de aplicación) y 128 (que difiere la transmisión de los datos hasta que las Partes contratantes afectadas encarguen a una autoridad de control nacional que ejerza un control independiente sobre el cumplimiento de los dispuesto en los arts. 126 y 127. Lo señalado en este artículo, a diferencia de los anteriores, si se aplica al Sistema de Información de Schengen).

Se consagra así que a iguales garantías, iguales excepciones.

Lo realmente relevante de este régimen de excepciones, y ahí estriba su potencialidad lesiva, es que no se limita a los principios de protección de los datos, sino que se extiende a los mecanismos de control independientes, ajenos a los concretos intereses públicos o privados, y que constituyen el mecanismo de la defensa de los intereses y de la salvaguarda de los derechos de los ciudadanos.

[113] Como caso paradigmático de esta superposición, puede señalarse el contemplado en el art. 115.1, cuando regula la creación de la autoridad de control encargada del control de la unidad de apoyo del S.I.S. : ".. El control se ejercerá de conformidad con lo dispuesto en el presente Convenio, en el Convenio del Consejo de Europa de 28 de enero de 1981..., teniendo en cuenta la Recomendación R (85) de 17 de septiembre del Comité de Ministros del Consejo de Europa... y con arreglo al Derecho nacional de la Parte Contratante responsable de la unidad de apoyo técnico ". La cursiva es nuestra.

[114] La unificación, más que en el sentido positivo de homogeneización de criterios, debe entenderse aquí en el sentido de una auténtica reformatio in peius.

Para concluir, no olvidemos que el Convenio sólo exige una armonización de las normas técnicas del Sistema Informático, tal y como se desprende del *párrafo 2 del art. 92* [115].

3.2. *Principios relativos a la protección de los datos personales.*

Los principios de protección de los datos personales deben aplicarse a todos los tratamientos de datos personales. Dichos principios tienen su expresión, por una parte, en las distintas obligaciones que incumben a los órganos o autoridades que efectúen tratamientos - obligaciones relativas, en particular, a la calidad de los datos, seguridad técnica, notificación a las autoridades de control, fundamentos de los tratamientos - y por otra parte, en los derechos otorgados a las personas, cuyos datos serán objeto de tratamiento, de ser informados acerca de tales datos, de poder acceder a ellos, de solicitar su rectificación o incluso de oponerse a su tratamiento.

El articulado del Convenio manifiesta la alegación de una serie de principios de protección de los datos personales, lo cual no prejuzga una regulación o contenido satisfactorios de los referidos principios. Estos principios aparecen diseminados a lo largo de su articulado, en un intrincado laberinto de denominaciones y menciones. Incluso, un mismo principio se menciona de formas diversas, cuando realmente hace referencia a lo mismo.

Ha sido por lo tanto necesario acometer una labor de sistematización y de reconstrucción de ese "puzzle" normativo. Este desorden evidencia el carácter asistemático y de "avanzar como impulsos" que presenta la regulación de la protección de los datos personales. Ello no es más que la consecuencia de la introducción tardía de estas cuestiones en el texto del Convenio, y de haberlo hecho con escasa confianza respecto a su eficacia.

3.2.1. Principio de Especificación de la Finalidad. Principio de Restricción de Uso.

El objeto de la recogida de datos personales debe determinarse; esto es, la finalidad de la recogida y la utilización de los datos deberá definirse de la manera más concreta posible. Una definición o una descripción vagas del objeto del tratamiento no es acorde con este principio, que constituye un mecanismo de salvaguarda importante, impidiendo una desviación, abuso o un uso torticero de los datos personales.

Con referencia al Convenio, debe indicarse que este principio no se cumple, pese a que se hace alegación del mismo, en la primera aparición que hace en el texto.

Proclamado en el *apartado 5* del *art. 38*, referente a las solicitudes de asilo, cuando se establece que los datos intercambiados únicamente podrán utilizarse

[115] Un estudio más pormenorizado acerca de los distintos ordenes normativos y su papel en la regulación de los datos personales puede encontrarse en: SÁNCHEZ BRAVO, A., "La protección de los datos personales...", cit., especialmente pp. 1424-1430.

para los fines previstos en el apartado 1, su determinación queda relegada a lo que establece el referido precepto [116].

Precepto cuya amplitud es manifiestamente desorbitante, no sólo desde el punto de vista material - de sus contenidos -, sino desde el punto de vista subjetivo. Cualquier Parte podrá " comunicar " a cualquier otra parte que lo solicite (ámbito subjetivo) las informaciones que posea acerca de.... y que sean necesarias para.... (ámbito material).

Como vemos los datos no sólo podrán utilizarse para el examen de una concreta solicitud de asilo, sino que también se posibilita un uso generalizado, y creemos que indiscriminado, amparándose en el cumplimiento genérico de las obligaciones del Capítulo; relativo a la responsabilidad del examen de las solicitudes de asilo.

Proclamado en el *art 32* [117] que cada Parte contratante examinará conforme a su derecho interno las solicitudes de asilo, ello implicará que será cada Estado miembro el que determinará unilateralmente que datos son necesarios, de acuerdo a su peculiar legislación, para un correcto examen de la solicitudes de asilo. Si a ello unimos el amplio elenco de datos [118] que podrán tratarse con este objeto,

[116] "1. Cada Parte Contratante comunicará a toda otra Parte Contratante que lo solicite las informaciones que posea acerca de un solicitante de asilo y que sean necesarias para:
- determinar la Parte Contratante responsable del examen de la solicitud de asilo;
- el examen de la solicitud de asilo;
- el cumplimiento de las obligaciones derivadas del presente Capítulo...
...5. Los datos intercambiados únicamente podrán utilizarse para los fines previstos en el apartado 1... ".

[117] "La Parte Contratante del examen de la solicitud de asilo lo llevará a cabo con arreglo a su Derecho nacional".

[118] El art. 38.2 hace referencia, de forma sorprendente y parece que irónicamente, a que "los datos sólo podrán referirse a:". La enumeración es extremadamente exhaustiva, conteniendo supuestos de discrecionalidad e indeterminación lesivos y peligrosos, y como casi siempre en detrimento de los derechos de los ciudadanos. Así puede citarse la letra c., donde después de enumerar en letras anteriores toda una serie de datos personales, posibilita que puedan comunicarse datos relativos a "los demás elementos necesarios para identificar al solicitante", consagrando un supuesto de absoluta discrecionalidad.

Así se expresa la enumeración de las referidas categorías de datos: "2. Dichos datos sólo podrán referirse a:

a. la identidad (nombre y apellidos, en su caso apellido anterior, apodos o seudónimos, lugar y fecha de nacimiento, nacionalidad actual y anterior del solicitante de asilo y, en su caso, de los miembros de su familia);
b. los documentos de identidad y de viaje (referencia, período de validez, fechas de expedición, autoridad que los haya expedido, lugar de expedición, etc.);
c. los demás elementos necesarios para identificar al solicitante;
d. los lugares de estancia y los itinerarios de viaje;
e. los permisos de residencia o los visados expedidos por una Parte Contratante;
f. el lugar en que se haya presentado la solicitud de asilo;
g. en su caso, la fecha de presentación de una solicitud de asilo anterior, la fecha de presentación de la solicitud actual, el estado actual del procedimiento y el contenido de la decisión adoptada."

observamos como este principio se difumina y disuelve en ese marasmo de remisiones y vacíos normativos.

Iguales criterios se establecen en el *art. 102* [119] respecto a la determinación de la finalidad en el uso de las categorías de datos señalados en los arts 95 a 100. Lo ya apuntado anteriormente cuando estudiamos la formulación y amplitud de estas descripciones, obvia cualquier otro comentario. Tampoco en este supuesto se salvaguarda este principio [120].

Más sorprendente resulta la regulación que se establece en la *letra a. del apartado 3 del art. 126* [121], cuando, tras proclamarse la salvaguarda del principio de especificación de la finalidad, se excepciona rápidamente recogiendo la posibilidad de utilizar los referidos datos con fines distintos. El recoger esta excepción abre las puertas a toda una serie de usos de diferente etiología, que consecuentemente escaparán a todo control, y por supuesto a todo conocimiento de los afectados. Además se formula de una manera genérica, amplia, sin establecer la más mínima cortapisa material respecto a las diferentes finalidades a las que potencialmente tal desviación pueda tender [122].

Eso sí, nuevamente el Convenio pretende adornarlo con un requisito formal, consistente en el previo acuerdo o consentimiento entre Estados, y en la adecuación a sus legislaciones internas. Las peculiares materias y tareas que contempla el Convenio (terrorismo, crimen organizado, armas, etc.) hace que esta posibilidad abra un amplio campo para el tratamiento de datos personales, como un elemento para luchar contra todas conductas o situaciones que puedan tener una conexión con las referidas materias. No debe olvidarse, por otra parte, que la mayoría de las legislaciones internas contemplan un generoso régimen de excepciones de las garantías, en el supuesto de tratamiento de datos personales realizados por los diferentes Cuerpos y Fuerzas de Seguridad del Estado.

Cuando de lucha contra el crimen y la delincuencia organizada estamos hablando, que Parte negará a otra que haga un uso diferente de los datos que originariamente le transmitió, si con ello lograra hacer frente a los ataques al " orden y/o la seguridad públicos ".

Este principio de especificación de la finalidad aparece conectado, como si del reverso de una misma moneda se tratara, con el *principio de restricción de uso.*

Si el tratamiento automatizado de los datos personales para ser leal y lícito debe contener la indicación previa de las finalidades a las cuales se dirige, ello implica la consagración efectiva de un uso restrictivo de aquellos por parte de las personas u órganos autorizados a utilizarlos [123].

Por tanto, el tratamiento debe referirse a datos pertinentes y no excesivos en relación con los objetivos perseguidos; objetivos que como ya se han indicado deben ser legítimos y explicitados previamente. De nada serviría que se exigiera, por parte de la legislación reguladora, el respeto del principio de especificación de la finalidad, si paralelamente no se limitara el uso que de los datos pueda hacerse.

En dos grupos pueden clasificarse las menciones que respecto a este principio realiza el Convenio:

a) Restricción de Acceso. Intenta garantizar que sólo las autoridades competentes y para el cumplimiento de específicas tareas tengan acceso a un determinado conjunto de datos personales:

1. "Los usuarios podrán consultar únicamente los datos que sean necesarios para el cumplimiento de su misión" (*Art.101.3*) [124].

[119] "Las Partes Contratantes sólo podrán utilizar los datos previstos en los artículos 95 a 100 con los fines enunciados para cada una de las descripciones mencionadas en dichos artículos."

[120] Y no puede hacerlo, por que a renglón seguido establece dos posibilidades ciertamente contradictorias con el principio que proclama:

1. Posibilidad de duplicar los datos, amparándose, eso sí, en "razones técnicas".

2. Posibilidad de pasar de una descripción a otra cuando así lo exijan, por enésima vez, "el orden y la seguridad públicos, una amenaza grave o la prevención de una amenaza grave".

Todo ello, cuando al final proclama "solemnemente ":

"Toda utilización de datos que no sea conforme con los apartados 1 a 4 se considerará como una desviación de la finalidad respecto al Derecho nacional de cada Parte Contratante".

Paradójicamente se habla de desviación de poder, cuando ésta se incluye en la propia regulación. Será "otra" desviación de poder.

[121] "3. a) La Parte contratante destinataria únicamente podrá utilizar los datos para los fines previstos en el presente Convenio para la transmisión de dichos datos; la utilización de los datos con fines distintos sólo será posible previa autorización de la Parte Contratante que transmita los datos y en cumplimiento de la legislación de la Parte contratante destinataria; podrá concederse la autorización siempre y cuando el Derecho nacional de la Parte Contratante que transmita los datos lo permita."

[122] La Comisión de las Comunidades Europeas estableció, a este respecto, en su Propuesta modificada de Directiva de 1992 que: "Una modificación posterior de la finalidad de un tratamiento sólo será legítima en la medida que sea compatible con la finalidad principal... En la medida en que la finalidad de la conservación y utilización de datos personales debe ser legítima, las finalidades potenciales de un tratamiento son limitadas. Dicho tratamiento sólo puede crearse y utilizarse para un objeto que se ajuste a las disposiciones de la Directiva y de las legislaciones nacionales de los Estados Miembros."

[123] Sobre este particular el propio Convenio establece: "4. Cada Parte Contratante facilitará al Comité Ejecutivo la lista de las autoridades competentes que estén autorizadas a consultar directamente los datos integrados en el Sistema de Información de Schengen. En dicha lista se indicará, para cada autoridad, los datos que puede consultar y para que misión. " (Art. 101.4)

[124] Este mismo precepto en sus párrafos 1 y 2 procede a la enumeración de los referidos usuarios:

"1. El acceso a los datos integrados en el Sistema de Información de Schengen, así como el derecho de consultarlos directamente, estará reservado a las autoridades competentes para:

a. los controles fronterizos;

b. las demás comprobaciones de policía y de aduanas realizadas dentro del país, así como la coordinación de las mismas.

2/ "Los datos únicamente podrán ser utilizados por las autoridades judiciales, los servicios y los órganos que realicen una tarea o cumplan una función en el marco de los fines contemplados en la letra a" (*Art. 126.3.b*).

b) Restricción de Uso. Pretende articular garantías para que el uso de los datos se haga de acuerdo con las finalidades previamente determinadas:

1/ "Los datos no podrán ser utilizados con fines administrativos. Como excepción, los datos introducidos con arreglo al artículo 96 sólo podrán utilizarse, de conformidad con el Derecho nacional de cada Parte Contratante, para los fines que se definen en el apartado 2 del artículo 101" (*Art. 102.4*).

Nuevamente se observa la derogación casi automática de la garantía que el precepto pretende establecer, y se lleva a cabo de una forma embrollada, demostrando una manifiesta ausencia de técnica legislativa, mediante la remisión a otros preceptos del Convenio.

Tal posibilidad podrá aplicarse a aquellos datos relativos a extranjeros incluidos en la lista de no admisibles (art. 96), y para el cumplimiento de comprobaciones de policía y de aduanas realizadas dentro del país, así como para la coordinación de las referidas actividades.

Parece consagrarse la equiparación entre infracciones penales y administrativas con respecto al tratamiento de los datos personales. Aun cuando se utilicen, apartándose de la finalidad original, no deben servir para arrojar más elementos de culpabilidad o de sospecha sobre los individuos afectados.

El dejar el control de esta posibilidad a la legislación de los Estados Miembros puede producir soluciones de lo más diverso, por cuanto el cumplimiento o no de determinadas formalidades administrativas implicará la introducción automática del extranjero en la lista de no admisibles, o bien simplemente se le pedirá la subsanación de tal falta en tiempo y forma oportunos.

La calificación de una persona como deseable o indeseable puede quedar limitada al cumplimiento de determinados requisitos formales, obviando las peculiares situaciones personales, familiares, culturas o políticas que coadyuven a la determinación de su particular estado y circunstancia. Lo contrario es reducir al hombre a un mero objeto de procedimiento, y no considerarlo sujeto del mismo.

2. Además, el acceso a los datos introducidos de conformidad con el artículo 96, así como el derecho a consultarlos directamente, podrán ser ejercidos por las autoridades competentes para la expedición de visados, por las autoridades centrales competentes para el examen de las solicitudes de visado y por las autoridades competentes para la expedición de permisos de residencia y para la administración de los extranjeros en el marco de la aplicación de lo dispuesto en el presente Convenio sobre la circulación de personas..."

2/ "La Parte Contratante destinataria sólo podrá utilizar los datos para los fines indicados por la Parte Contratante que los proporcione, y deberá hacerlo cumpliendo las condiciones impuestas por dicha Parte Contratante" (*Art. 129.a.*).

La articulación de este principio, que se incardina en un precepto general relativo a la transmisión de los datos, se hace recaer sobre el acuerdo entre Estados. Será la Parte transmisora la que señalará tanto las finalidades como las condiciones de uso a las que deberá ceñirse la Parte receptora. Ahora bien, no siempre será posible esa adecuación. Y no lo será por que no se quiera, sino simplemente por que no se pueda; por que la legislación interna del Estado receptor le impida o dificulte el cumplimiento de ciertas condiciones, o bien por que regule supuestos no contemplados en su norma patria. La situación se agravaría si nos encontramos con Estados que no posean una norma interna reguladora de la protección de los datos personales automatizados.

Además, se echa de menos el establecimiento de un mecanismo de garantía efectivo que asegure esa adecuación. ¿ Como un Estado soberano va a poder controlar el uso que internamente otro Estado, también soberano, ha hecho de determinados datos, aunque aquel se los haya transferido ?; aun cuando fuera posible, ¿como controlar, y mucho menos evitar o impedir, determinados usos desviados? Preguntas, ciertamente, de difícil resolución.

Si como parece establecer el Convenio, se tiende a un espacio único, a una legislación única por que no se han establecido unas normas unificadas para regular el flujo de datos entre Estados Partes, máxime cuando de transmisión de datos estamos hablando.

Ello nos conduce a formularnos otras preguntas. ¿ Que resultado se deduciría de un eventual incumplimiento por el Estado receptor ?; ¿ de acuerdo a qué legislación se deduciría tal responsabilidad ?, ¿ podría imponerse una sanción ?; ¿ de qué naturaleza ?. Preguntas sin respuestas en el Convenio.

La salvaguarda de la autonomía nacional condena a estas correctas declaraciones, al menos en lo que de deseo expresan, al papel de meras expresiones grandilocuentes, vacías de contenido.

3.2.2. Principio de Calidad de los Datos.

La naturaleza de los datos debe corresponderse con el objetivo perseguido. Ello implica que los datos deberán ser adecuados, pertinentes y no excesivos con relación a los fines que se persiguen. Los datos deben ser exactos y, cuando sea necesario, deben actualizarse. En el supuesto de que hubiera datos incorrectos o incompletos con respecto a los fines para los que fueron recogidos, debe preverse la posibilidad de su supresión o rectificación.

La calidad de los datos supone el criterio protector genérico, en torno al cual se articulan una serie de garantías, que contribuyen a perfilar su concreto contenido.

Pero criterios como la pertinencia, la exactitud o cualquier otro, no deben entenderse aisladamente, sino que forman parte integrante de esa calidad, de esa esencia misma de los datos personales.

Este principio supone la consagración de un criterio objetivo, sin cuya escrupulosa concurrencia no deben nunca ser objeto de tratamiento automatizado los datos personales. La calidad se perfila así en su acepción negativa, pues se predica en lo que de garantía tiene para los ciudadanos, y no de la "calidad" que deben de reunir determinados datos para posibilitar su tratamiento. La concurrencia de sus contenidos supone una protección, no una habilitación a los agentes que tratan los datos para que procedan a tal operación.

Volviendo al contenido del Convenio, de este tenor se expresa el *párrafo 6* del *artículo 38* [125]:

"La Parte Contratante que transmita los datos velará por su exactitud y su actualidad. En el supuesto de que dicho Estado miembro facilitara datos inexactos o que no hubieran debido transmitirse, se informará inmediatamente de ello a las Partes Contratantes destinatarias, las cuales estarán obligadas a rectificar dichas informaciones o a eliminarlas." [126].

La eficacia de este principio se articula, como se extrae del propio precepto, en torno a un doble principio:

1. La Parte que transmita los datos debe, y aunque nada dice el texto debe entenderse que antes [127] y durante la transmisión, velar por la exactitud y la actualidad de los datos. Pero su responsabilidad no finaliza ahí. Si efectuada la transmisión se evidencia que los datos son incorrectos o no pertinentes debe comunicarlo *inmediatamente* a la Parte contratante que los hubiera recibido. Sorprende como al Estado transmisor, causante del error, sólo se le exige un deber de comunicación, y no cualquier otra conducta que tienda a evitar o al menos atenuar los resultados perniciosos que de un uso no correcto de los datos personales puedan derivarse.

Podrá objetarse que los datos están en poder de un tercer Estado, con lo cual escapan al control del Estado transmisor; por otra parte, ese tercer Estado puede haber hecho uso de los datos recibidos de " buena fe ", antes de recibir la comunicación de que los datos son incorrectos o no pertinentes, y consecuentemente después de haberse generado un perjuicio para los individuos afectados.

¿ En que puede concluir este galimatías ? La solución parece ser una exoneración de responsabilidad por parte de los Estados intervinientes, unos por que cuando comuniquen los defectos que sufren los datos, tal vez ya se haya hecho uso de ellos; los otros por que han procediendo a la utilización de los datos confiando en su regularidad [128]. Serán los individuos afectados los que sufran las consecuencias. Volveremos sobre esta cuestión posteriormente al abordar el estudio del Principio de Responsabilidad por Infracción.

2. La Parte que reciba los datos deberá, si por la Parte transmisora se le comunica que los datos son incorrectos o no pertinentes, proceder inmediatamente y "*ex officio*" a su rectificación o cancelación. Nada indica el precepto si tales fallos son constatados por la Parte receptora de los datos; es decir si constata tales deficiencias antes de hacer uso de los mismos. La solución nos la proporciona el propio Convenio cuando señala el deber de informar a la Parte informadora, la cual procederá inmediatamente a la comprobación de las posibles deficiencias, y constatadas éstas debe proceder a la rectificación o cancelación de los datos [129].

Supone la otra manifestación del fenómeno estudiado anteriormente, si bien aquí, regulado con evidente acierto. Creemos que constituye un efectivo remedio

[125] Centramos el estudio en este precepto por ser de contenido idéntico al resto de los que se refieren a este principio, presentando una problemática idéntica, que es la general del Convenio. Al resto de preceptos se irá haciendo referencia en el desarrollo de nuestro viaje por este principio.

[126] En iguales términos se expresa el artículo 126.3.c., si bien aquí consagra una importante novedad digna de reseñar. Las comprobaciones acerca de la calidad y de la exactitud de los datos no sólo se deja a la Parte transmitente, si no que también la persona interesada podrá solicitar que se proceda a tal verificación de calidad. Esta posibilidad directa para los individuos constituye un notable acierto del Convenio, pues implica el dotar a los interesados de la posibilidad de conocer que existe un tratamiento automatizado sobre sus datos personales, y además cual es el contenido exacto, tanto del proceso, como de los mismos datos. Incorpora el reconocimiento a los afectados de su derechos de acceso, rectificación y cancelación sobre sus datos personales. Supone una consagración de ese derecho a la libertad informática.

[127] Esta afirmación tiene apoyatura en el hecho de que el propio Convenio exige a las Partes Contratantes que se proceda a la verificación de exactitud y actualidad de los datos en el momento de la introducción de los datos en el S.I.S., y por supuesto, en un momento anterior a que la transmisión de datos a otros Estados se efectúe. Se recoge la posibilidad de un control interno, previo por y para cada Estado, que tendrá como límite inexcusable el momento en que se proceda a la introducción de los datos en el Sistema común. Control que de no efectuarse deparará las responsabilidades a que haya lugar.

Así se expresa el Art. 105: "La Parte Contratante informadora será responsable de la exactitud, actualidad y licitud de la introducción de los datos en el Sistema de Información de Schengen."

[128] Si se establece la posibilidad de un conflicto entre Estados miembros en torno a la concurrencia o no de errores de hecho o de derecho que desvirtúen esa calidad que de los datos deba predicarse; ello no implica que exista un conflicto en torno a la delimitación o atribución de responsabilidades. Se trata de un conflicto anterior a la eventual depuración, y por tanto atribución de responsabilidades. Los Estados discrepan acerca del contenido de los datos, no de las consecuencias derivadas de un uso o transmisión posterior.

El párrafo 3 del art. 106 así se expresa: "Si las Partes Contratantes no pudieran llegar a un acuerdo, la Parte Contratante que no hubiere dado origen a la descripción someterá el caso para dictamen a la autoridad de control común mencionada en el apartado 1 del artículo 115."

[129] De esta manera se expresa el Art. 106 en su párrafo 2: "Si una de las Partes Contratantes que no haya hecho la descripción dispusiera de indicios que hagan presumir que un dato contiene errores de hecho o de derecho, informará de ello lo antes posible a la Parte Contratante informadora, la cual deberá comprobar la comunicación y, en caso necesario, corregir o suprimir sin demora el dato."

para evitar perniciosos efectos o consecuencias para los ciudadanos, derivados de una falta de diligencia por parte de los Estados Miembros, cuando procedan al tratamiento de sus datos personales. Observamos como el precepto que venimos estudiando hace referencia a dos categorías que engloban ese principio genérico de la calidad pero que no obstante no deben confundirse. Aunque complementarios, no pueden identificarse, pues responden a dos presupuestos diferentes:

a) Contenido Material: Datos Exactos.
b) Contenido Temporal: Datos Actuales.

Así datos exactos en este momento, devendrán inexactos por el transcurso del tiempo y por las variaciones de las circunstancias en las que se apoyan debido a ese caminar del tiempo. Igualmente la afirmación del carácter actual de los datos, no prejuzga su exactitud.

El estudio que estamos realizando vuelve a complicarse cuando, con respecto a las obligaciones de los Estados referentes a la salvaguarda de los datos, se hace referencia, por un lado a *datos inexactos*; y por otro a una nueva categoría: *datos que no hubieran debido transmitirse.*

Para nada se hace mención a la otra categoría: la actualidad. No se hace referencia a datos " antiguos ", " no actualizados ", o cualquier otra mención semejante.

Bien pudiera entenderse que aparecería englobada en la categoría de datos que no debieron transmitirse, pero eso mismo podría predicarse de la exactitud. La conceptuación de un dato como no transmisible es una consideración genérica que engloba aquellos supuestos en que los datos no presentan la calidad suficiente para ser transmitidos, independientemente de que sea por falta de exactitud o de actualidad.

La referencia es a un criterio objetivo, previo, genérico - el carácter intransmisible de los datos -, y no a una cualidad concreta de los datos - la actualidad.

No se acierta a comprender esta diferenciación. Acaso nos encontremos ante un "*lapsus legislatoris*" o realmente se pretenda hacer referencia a algo diferente. Baste ahora indicarlo.

Para concluir, debemos hacer referencia a otro criterio, que aunque no explicitado en el texto del Convenio, si puede deducirse del mismo. Este es la *integridad* de los datos.

La salvaguarda de un correcto uso de los datos personales debe incluir el que los datos sean utilizados en su integridad, tanto de manera formal como material. Es decir, en lo referente a su expresión en los textos o documentos que le

sirven de soporte, y en el contenido concreto que con los referidos datos se pretende expresar.

La apelación a la integridad en la utilización de los datos, no debe entenderse como un propuesta a favor de la utilización masiva de los mismos, sino todo lo contrario. Lo que se pretende salvaguardar es una utilización racional y no parcelada, que impida una versión desvirtuada de los hechos y de las circunstancias que confluyen en las personas. En muchas ocasiones será más lesivo, para el ejercicio y disfrute de los derechos, un uso parcial o una imagen parcial de una determinada situación, que un uso no estrictamente correcto de los datos.

Los datos en su utilización deben atemperarse al criterio de la integridad, para posibilitar así un conocimiento completo y unos efectos también completos; entendidos estos últimos como garantías para los afectados.

No debe tolerarse que un aspecto parcial se equipare al conjunto; que una persona quede reducida a la manifestación concreta de un aspecto de su personalidad.

En el Convenio, de manera indirecta como ya indicamos, se recoge el principio de integridad cuando establece que será la Parte informadora la única autorizada para completar los datos que hubiera introducido [130].

De lo expresado parece deducirse que podrán introducirse datos incompletos, de ahí que sea necesario otorgar esta facultad "reparadora" a los Estados.

Lo que debería haberse establecido es la prohibición absoluta de tratar datos incompletos, por el perjuicio que puede deparar para los afectados. Además esta facultad de completar los datos no se concede al resto de Partes Contratantes, si apreciaran una deficiencia en el contenido de los datos, sino que sólo se otorga a la Parte informante. Se aparta así del criterio señalado anteriormente con respecto a la posibilidad de modificación de datos inexactos o que no hubieran debido transmitirse.

3.2.3. Principio de Conservación Limitada de los Datos.

La conservación de los datos personales en una forma que permita la identificación del interesado, sólo debe quedar autorizada durante un período que no exceda del necesario para los fines para los que fueron registrados. Esta limitación pretende garantizar lo que se ha denominado *derecho al olvido.*

Los datos deben tener una vigencia estricta, en lo afectante a su uso y transmisión, para impedir que situaciones concretas y circunstanciales, supongan un elemento de estigmatización social para los afectados.

[130] Cfr. Art. 106.1.

Constituye un medio de poner freno a ese afán devorador de datos que presentan actualmente, tanto las administraciones públicas, como grandes multinacionales de los sectores de comunicación e información.

En el Convenio, también se recoge este principio en la forma que venimos señalando [131], estableciendo un procedimiento de verificación y examen respecto a la necesidad de conservar los datos.

Siendo capital el reconocimiento del principio, su efectividad se manifestará en el mecanismo que se ponga en práctica para aplicarlo a los supuestos concretos que se presenten, así como las actuaciones que deberán desarrollar las autoridades u órganos encargados de la conservación.

La regulación a este respecto es bastante dispar, atendiendo a un doble criterio: datos referentes a personas y cualesquiera otros datos. Esta diferenciación genera importantes diferencias respecto al período máximo de examen y conservación de las diferentes categorías de datos.

a. Datos referentes a personas.

Si de datos personales referentes a solicitantes de asilo se trata, el Convenio no establece ningún criterio respecto al período máximo de conservación de los datos [132], y ni siquiera se hace referencia a un plazo razonable para proceder al examen de la oportunidad o no de conservar los datos.

El haber regulado estos datos como una categoría especial, aparte, con su peculiar régimen de garantías, hace que en este caso la desprotección y la arbitrariedad sea máxima. ¿ Como puede establecerse una regulación con semejante deficiencia, cuando de asilo, de desarraigo familiar, social y cultural, estamos hablando ?. Quizás por eso, por que no se espera una crítica, ni siquiera una súplica, de "unos pobres sin hogar".

De esta manera se expresa el Convenio, a este respecto:

"La Parte Contratante de que se trate estudiará a su debido tiempo la necesidad de conservarlos." [133].

[131] "Los datos transmitidos se conservarán durante un período no superior al necesario para los fines para los que se hubieren intercambiado..." (Art. 38.9).
"Los datos de carácter personal introducidos en el Sistema de Información de Schengen a efectos de la búsqueda de personas sólo se conservarán durante el tiempo necesario para los fines para los que se hubieren facilitado los datos..." (Art. 112.1).

[132] En ningún caso debe ser superior a la conclusión del examen de una solicitud de asilo, y por tanto a su resolución.

[133] Art. 38.9

Como indicamos, más indeterminación es imposible. ¿Que entender por su debido tiempo? Creemos que aquí sí la respuesta es clara: cuando los Estados quieran, con absoluta independencia.

Mejor y más completa es la regulación que se establece respecto a los datos referentes a personas incluidas en las categorías señaladas en los arts. 95 a 99 [134].

Tampoco se establece un período máximo de conservación, pero lo que sí se incluye es el plazo en el cual deberá procederse al examen para determinar la necesidad de conservar los datos. El plazo general es de 3 años, que queda reducido a 1 en el supuesto de datos relativos a personas a efectos de vigilancia discreta o de control específico. Este plazo comienza a correr desde el momento de introducción de los datos.

Pero lo realmente relevante de esta regulación es que constituye un mínimo inexcusable. Aquí los Estados no podrán obviar estos plazos, y ello en virtud de dos criterios:

1. Los Estados no podrán ampliar este período. *A sensu contrario*, lo que si podrán es establecer unos plazos más cortos para efectuar dicho examen.
2. La Unidad de Apoyo Técnico del S.I.S. procederá, en caso de que los Estados no le comuniquen el mantenimiento de la descripción, a la supresión de los datos. Esta supresión se comunicará con un mes de antelación a la Parte Contratante afectada. Esta supresión automática es una importante novedad, que garantiza que los Estados no puedan mantener *sine die* la descripción en el Sistema, alegando que no se han cuestionado la necesidad o no de conservación.

Como venimos señalando, estas garantías no impiden que la descripción siga manteniéndose, si el Estado informador considera que sigue siendo necesaria para el cumplimiento de los fines que motivaron su introducción [135]. El mantenimiento implica que nuevamente vuelve a correr el plazo de 3 años, o de 1 en su caso, a cuya conclusión deberá procederse a un nuevo examen. La Unidad de Apoyo Técnico deberá ser informada de este mantenimiento.

b. Datos referentes a objetos. [136]

A diferencia de las categorías anteriores, estos datos están sujetos a un período máximo de conservación, sin necesidad de una actividad de examen por parte de los Estados miembros acerca de la necesidad o no de conservación de los datos.

[134] Art. 112.

[135] Vid. lo ya señalado anteriormente respecto a la problemática que plantea el Convenio respecto a la delimitación de las finalidades que motivan el tratamiento automatizado y uso de los datos personales.

[136] Art. 113.

La eliminación se produce de manera automática, una vez transcurrido el período de vigencia de los datos.

El tiempo máximo de conservación se determina en cascada:

1. Se conservarán durante un período máximo de 10 años los datos distintos de los mencionados en el *artículo 112*. Deberán incluirse los datos personales, no incluidos en la categoría anterior, que se transmitan para la comprobación de una descripción de un objeto encontrado [137].
2. Como máximo durante 5 años, los datos relativos a documentos de identidad expedidos y billetes de banco registrados.
3. Los referentes a vehículos de motor, remolques y caravanas, como máximo durante 3 años.

Estos datos suprimidos se conservarán durante un año más en la Unidad de Apoyo Técnico, con el sólo fin de consultarlos para comprobar *a posteriori* su exactitud y la licitud de su integración.

3.2.4. Principio de Responsabilidad por Infracción.

Antes de proceder al tratamiento automatizado de los datos, debe especificarse en las legislaciones correspondientes que el Estado será responsable de los perjuicios que ocasione. Se trata de una obligación positiva que deben asumir los Estados. Para los individuos, supone el concederle un ámbito de protección y de restitución en sus legítimos derechos e intereses que hayan podido verse afectados por el tratamiento en forma automatizada de sus datos personales.

Y es una consecuencia que no debe extraerse del proceso global de tratamiento, ni considerarse sólo como un derecho de los afectados. Es una de las posibles consecuencias del proceso de tratamiento, y por lo tanto debe estudiarse unitariamente en el mismo.

Las Partes contratantes serán responsables de cualquier daño ocasionado a una persona como consecuencia de la explotación de su parte nacional del S.I.S. [138]. Esta responsabilidad se determinará en cada Estado de acuerdo a su Derecho interno. Ello implica que se producirán disfuncionalidades en este sistema de atribución de responsabilidades. Conductas que en un Estado serán consideradas como causa de responsabilidad, en otro no lo serán. Incluso en aquellos en que lo sea de manera igualitaria, su nivel de intensidad variará considerablemente. No debe olvidarse que este principio no se recoge en todas las legislaciones internas que para la protección de los datos se han promulgado en los Estados miembros [139].

[137] Art. 100.2. Cfr. HEREDERO HIGUERAS, M., "La protección de los datos personales en manos de la policía..." cit., p. 40.

[138] "Toda Parte Contratante será responsable, con arreglo a su derecho nacional, de cualquier daño ocasionado a una persona como consecuencia de la explotación del fichero nacional del Sistema de Información de Schengen..." (Art. 116.1).

Creemos que hubiera sido más conveniente el regular una responsabilidad general, conjunta, pues de una organización y actividades conjuntas estamos hablando; y dejar a los Estados Miembros las concretas formas de satisfacción a los administrados por los perjuicios irrogados de acuerdo a sus peculiares instituciones y a su tradición jurídica.

El ámbito de responsabilidad incluye todos los que daños que se irroguen a una persona. Criterio ciertamente amplio del que precisamente tampoco podrá hacerse un uso desmesurado o no acorde con la peculiar naturaleza de la institución. Estos daños deben ser consecuencia de la explotación de la parte nacional del Sistema, y por lo tanto deben incluirse cualquier operación o conjunto de operaciones aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción [140].

Ya indicamos anteriormente que en esta cuestión de atribución de responsabilidades los principales obstáculos podrían derivar de un enfrentamiento entre Estados miembros en orden a cual corresponde tal responsabilidad, y quien debe, consecuentemente, hacer frente a las prestaciones que se deriven del daño causado.

El Convenio hace frente a esta cuestión estableciendo unos criterios de determinación del Estado responsable:

a) La asunción de responsabilidad corresponde como regla general a todo Estado Miembro.
b) Si los daños son consecuencia de la transmisión de datos que contengan errores de hecho o de derecho, la responsabilidad será imputable a la Parte Contratante informadora. No obstante, la Parte que usó los datos transmitidos no podrá alegar que se le transmitieron datos incorrectos si, con arreglo a su Derecho interno, le corresponde la responsabilidad con respecto de una persona perjudicada [141]. Se trata de evitar que se produzca una elusión de responsabilidad alegando una eventual norma de conflicto, en menoscabo de una norma interna de carácter imperativo.

[139] Se recoge especialmente en Alemania y en España (art. 17 de la LORTAD). Vid. sobre ello: HEREDERO HIGUERAS, M., "La protección de los datos personales en manos de la policía...", cit., p.40.

[140] Tal como se recoge en el apartado b) del artículo 2 de 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..., cit., p. 38.

[141] Art. 126.3.d.

c) Si la demanda de responsabilidad se plantea contra la Parte Contratante destinataria y ésta viene obligada a reparar el perjuicio causado y a hacer frente a la correspondiente indemnización, la Parte Contratante informadora deberá, previa petición, proceder al reembolso integro de las cantidades satisfechas por la Parte destinataria. Este derecho de reembolso encuentra su limite en el supuesto de que la Parte destinataria, demandada, hubiese hecho uso de los datos incumpliendo el Convenio.

3.3. *Derechos de la persona interesada.*

Ante el tratamiento automatizado de sus datos personales toda persona debería poder:

— obtener a intervalos razonables y sin plazos o gastos excesivos, la confirmación de la existencia o no en el fichero automatizado de datos personales que le afecten, así como la comunicación de los mismos de forma inteligible,
— obtener, si hubiera lugar, la rectificación de dichos datos o su cancelación si hubieran sido tratados violando aquellas normas que aseguran y hacen efectivos los principios básicos de protección de los datos personales,
— disponer de un recurso si no se da curso a una solicitud de confirmación o, en su caso, de rectificación o cancelación.

Corresponde a los Estados miembros establecer como deben ofrecerse estas informaciones al interesado.

El *apartado 1* del *art. 109*, que regula el *derecho de acceso* [142], nos remite al Derecho nacional de la Parte contratante ante la que se hubiese alegado el derecho. Su ejercicio queda diferido hasta que la autoridad de control nacional establezca las modalidades en que deberá hacerse efectivo el derecho, si así lo prevé la legislación interna.

El derecho de acceso puede ejercerse previa solicitud. El interesado tendría derecho a obtener información sobre el origen y sobre la utilización de los datos personales en cuestión.

Cuando la solicitud de acceso se ejercite ante una Parte contratante que no haya realizado la descripción, aquella no podrá facilitar información respecto a

[142] "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 hubiese alegado tal derecho. Si el Derecho nacional así lo prevé la autoridad nacional de control prevista en el apartado 1 del artículo 114 decidirá si se facilita información y con arreglo a qué modalidades."
En idénticos términos se expresa el art. 127.2.c.: "el acceso a los datos y las condiciones en que se concederá dicho acceso estarán regulados por el Derecho nacional de la Parte Contratante a la que la persona interesada presente su solicitud."

los datos que se le solicitan. Supone una derogación de este derecho, que se ampara en la responsabilidad que corresponde a cada Estado por la introducción de descripciones en el Sistema. Además como ya vimos, según se desprende del art. 105, sólo la Parte Contratante informadora será responsable de la introducción de los datos, y consecuentemente ante ella debería ejercerse el derecho de acceso.

No obstante esta imposibilidad no presenta caracteres absolutos. Si se ha concedido a la Parte informadora la posibilidad de manifestarse respecto a dicha solicitud de acceso, la Parte destinataria si podrá conceder la información sobre los datos solicitados. Supone una manifestación, *mutatis mutandi*, del principio administrativo del silencio positivo.

Pero el derecho de acceso aparece limitado en su ejercicio. Corresponde a los estados Miembros decidir en qué medida deben incluirse estas excepciones, a no ser que vengan impuestas por el Convenio. Tal es el caso de las descripciones integradas con vistas a una vigilancia discreta, en el que se denegará siempre el derecho de acceso, al menos mientras no concluya tal actividad y se proceda a la modificación de la descripción [143].

La introducción de excepciones deben limitarse a aquellas que sean necesarias para la salvaguarda de los valores indispensables para una sociedad democrática, no siendo exhaustiva la relación de intereses que deben salvaguardarse.

Dos razones justifican tales excepciones:

→ 1. Cumplimiento de la tarea legal consignada en la descripción. Se exige el requisito suplementario de que el comunicar información al interesado pueda ser perjudicial para el cumplimiento de tal tarea. De ahí que, sí pese a comunicarse información, tal tarea legal no sufre perjuicio o menoscabo, no pueda en ningún caso negarse el derecho de acceso.

Las cuestiones fundamentales surgen al intentar determinar que sea dicha tarea legal. Para ello es necesario remitirse a cada una de la categorías de descripciones que se señalan en el Convenio (arts. 95-100), para determinar cual es la actividad a desarrollar por las autoridades y órganos competentes en cada supuesto. Cuestiones que tienen su referente en esa función general que no es otra que el preservar el orden y la seguridad públicos. De ahí que deban estimarse estas tareas en sus justos límites y con relación a cada supuesto concreto, y no establecer una generalización ampliadora, que olvida la naturaleza concreta del caso en cuestión y las también concretas medidas a aplicar.

[143] Se trata con ello de evitar que se entorpezca gravemente el cumplimiento de una función de investigación por los órganos policiales. Este interés que debe salvaguardarse no debe constituir, no obstante, una vía por la cual se pueda derogar el control que sobre sus propios datos debe otorgarse a los ciudadanos.

2. Protección de los derechos y libertades de terceros.

Al ser equivalente al derecho de acceso del interesado debe considerarse como un motivo válido para limitar este derecho. Aparte del ejercicio de los derechos fundamentales por terceros, deberán incluirse entre las causas que dan lugar a esta limitación las siguientes: secretos de negocios de terceros; normas del secreto profesional a que están sometidas las profesiones jurídicas o médicas; derecho de un tercero a elaborar su propia defensa; y la defensa de los derechos humanos.

Si el interesado no puede tener acceso a datos que le conciernen y que figuren en el fichero del S.I.S., la autoridad nacional de control debe, previa solicitud, proceder a las verificaciones necesarias para la comprobación de los datos y la licitud de los tratamientos y uso con relación a los fines para los que introdujeron los datos. El procedimiento se acomodará a lo establecido por la normativa interna del Estado ante el que se presente la solicitud. Si el Estado que introdujo los datos fuera otro diferente al que se ha presentado la solicitud, se exige una colaboración entre las autoridades de control de ambos Estados para proceder a tal control [144].

El *artículo 110* recoge el *derecho de rectificación y supresión o cancelación.* El derecho de rectificación se ejercerá sobre datos que contengan errores de hecho. El de supresión sobre aquellos que contengan errores de derecho. No creemos sea este el criterio más correcto para fundamentar el ejercicio de los derechos. Máxime cuando serán los hechos los que determinarán el Derecho aplicable; a tales circunstancias tal marco jurídico regulador. No se acierta a comprender el porqué de esta división artificiosa. Debería ser la intensidad del error, y su influencia en la valoración de las situaciones que se presenten, la que determinara la rectificación o la cancelación, y no la naturaleza del error. Debe ponerse el acento en las consecuencias del error y no en la etiología del mismo. En muchas ocasiones será una incorrecta apreciación de los hechos la que supondrá una mayor lesión, al otorgar a las personas una imagen desvirtuada y alejada de su realidad cotidiana. El Derecho vendrá después para establecer el régimen jurídico al que debe someterse e imponer, si así se establece, la sanción correspondiente.

El *derecho de ejercicio de acciones* se reconoce en el *artículo 111*. Se reconoce el Derecho a acudir ante los órganos competentes de los Estados miembros para solucionar los conflictos que pudieran plantearse con respecto al ejercicio de los derechos de información (acceso), rectificación, supresión o indemnización [145]. La distinción entre órganos jurisdiccionales y otras autoridades se debe, como señala Heredero, a la diversidad de los sistemas de control existentes en las legislaciones

[144] Art. 114.2 .
[145] Respecto al derecho de indemnización, vid. lo ya apuntado anteriormente cuando abordamos el estudio del principio de responsabilidad por infracción.

nacionales [146]. Corresponde a las legislaciones nacionales otorgar estas facultades de recurso a los interesados para permitirles que defiendan de una manera amplia todos los derechos que les reconoce el Convenio.

Esta protección de los interesados , y la resolución de las respectivas acciones, debe concluir, además de en una restitución en los derechos afectados, en que las demás Partes Contratantes reciban una notificación de rectificación, supresión o bloqueo de los datos con objeto de que puedan rectificar, suprimir o bloquear los datos en cuestión; tal y como se establece en el art.106.

3.4. *Autoridades de Control.*

En el marco del Convenio son varias las autoridades que pueden integrarse dentro de esta categoría. Ello se debe a la propia estructura funcional del Sistema, articulada alrededor de una Unidad Central y, a una Parte Nacional en cada Estado Miembro. También confluye el intento por preservar todos los intereses en conflicto; la salvaguarda de la autonomía de los Estados Miembros, el respeto por los derechos de las personas afectadas y la consecución de unos objetivos comunes.

Conviene señalar que la existencia en cada uno de los Estados Miembros de una autoridad nacional encargada de ejercer un control independiente sobre los datos personales constituye requisito previo e inexcusable para cualquier transmisión de datos personales, y por tanto para poner en marcha el propio Convenio [147].

Para una mejor comprensión de estos órganos, sistematizaremos nuestra exposición, aludiendo a los concretos perfiles que presenta cada uno.

3.4.1. Autoridad con competencia sobre la Parte Nacional del S.I.S. [148]

Es un órgano de naturaleza evidentemente técnica, que ostenta la competencia central sobre dicho fichero nacional y que desarrolla las siguientes funciones:

— Competencia exclusiva sobre la introducción de las descripciones. Será esta autoridad la que procederá a la introducción efectiva de los datos en el Sistema, cuando así le sea solicitado por los órganos judiciales y/o administrativos competentes, dependiendo de la naturaleza de la descripción que se pretenda. Igualmente le corresponderá la competencia para decidir acerca de la modificación de una descripción solicitada por otro Estado miembro [149], así como para la integración de descripciones[150].

[146] Cfr. HEREDERO HIGUERAS, M., "La protección de datos personales en manos de la policía...", cit., p. 42.
[147] Arts. 38.12 y 128.1
[148] Art. 108
[149] Art. 102.3
[150] Art. 107

— Será responsable del correcto funcionamiento de la Parte Nacional del Sistema. Supervisará que todas las operaciones realizadas por y en dicha Parte Nacional se hagan de acuerdo a los protocolos reglamentarios y técnicos establecidos por el Convenio, evitando usos indeseables o torticeros.
— Adopción de medidas necesarias para garantizar el cumplimiento del Convenio. Incluye las funciones organizativas, de material y equipos, así como todas las operaciones técnicas para asegurar una correcta y fluida comunicación entre la Unidad Central y la parte nacional del fichero.
— Organo de comunicación con los restantes Estados Miembros, en orden al funcionamiento del S.I.S.

Nada se dice acerca del nombramiento de dicha autoridad. Las funciones a desarrollar y su naturaleza, nos inducen a pensar que será un órgano nombrado por los Gobiernos de los Estados Miembros, como encargados gubernamentales de la parte que les corresponde en el S.I.S. [151].

3.4.2. Autoridad Nacional de Protección de los Datos. [152]

Se dispone el establecimiento en cada Estado Miembro de una autoridad de control independiente dotada de medios de investigación y de intervención. Aquellos Estados que aún no tengan esta autoridad deberán proceder a nombrarla, so pena de no poder participar en la transmisión de datos a través del S.I.S. Sus funciones fundamentales son:

— Ejercer un control independiente sobre el fichero de la Parte Nacional del S.I.S. Control referido a la licitud y legalidad de los tratamientos.
— Comprobar que el tratamiento y la utilización de los datos no lesionan los derechos de las personas afectadas. Constituye su función capital, y cuyo efectivo desarrollo o no evidenciará el grado de independencia que las legislaciones nacionales han otorgado a este órgano.
— Conocer de las acciones que, en los supuestos en que no estén atribuidas al conocimiento de autoridades judiciales, correspondan a las personas afectadas respecto a la titularidad, ejercicio y defensa de sus derechos de acceso, rectificación, supresión e indemnización.

La facultad de control tiene por objeto permitir a la autoridad de control que recabe de los responsables del tratamiento los datos necesarios para el cumplimiento de su cometido. Esta competencia se manifiesta en concreto en el acceso a los datos que son objeto de tratamiento. Acceso que deberá hacerse respetando la confidencialidad que a los datos concede el derecho interno, para respetar los derechos de las personas afectadas.

[151] La utilización de la expresión "designará", parece indicar un mayor quantum de vinculación con la actividad gubernamental. Nos remite más a una facultad exclusiva del Gobierno, que a un procedimiento de elección y posterior nombramiento.
[152] Art. 114

3.4.3. Autoridad de Control Común. [153]

Su introducción responde a la búsqueda de un elemento homogeneizador, aglutinante de esa unidad de acción y de objetivos que se pretende [154].

Su función primordial es efectuar un control sobre la Unidad de Apoyo Técnico del S.I.S. Control acerca de la legalidad y de la correcta ejecución de las disposiciones del Convenio, y de las actividades desarrolladas por la Unidad Central. Pero dicho control no podrá ejercerse de cualquier manera, sino teniendo en cuenta determinadas regulaciones protectoras de los datos personales, y concretamente el Convenio 108 y la Recomendación R (87) 15, ambas del Consejo de Europa.

Para el cumplimiento de esta misión estará facultada para acceder a los datos integrados en la Unidad de Apoyo Técnico. Este acceso se revela imprescindible para que dicha autoridad pueda ejercer correctamente su función, conociendo directamente los fallos y disfuncionalidades del sistema.

Esta función genérica se manifiesta en las siguientes atribuciones:

— Competencia para analizar las dificultades de interpretación y aplicación que surjan con la explotación del S.I.S. Se le atribuye competencia para la resolución de controversias entre Estados Miembros acerca de la existencia o no de errores en determinados datos que hayan sido objeto de transmisión [155]. Igualmente se le atribuye competencia para emitir un dictamen, si así se lo solicita alguna Parte Contratante acerca de las dificultades de interpretación y aplicación de las medidas contempladas en el art.126
— Procederá al estudio de los problemas que pudieran surgir en el ejercicio del derecho de acceso y del control independiente efectuado por las autoridades nacionales de protección de datos. Estos estudios y la efectiva consideración de sus conclusiones pueden contribuir a constituirlo de manera indirecta en una especie de "segunda instancia" para la protección de los datos, al poner de manifiesto las trabas planteadas por la aplicación de las legislaciones nacionales e indicar los nuevos caminos por los que seguir avanzando.
— Elaboración de propuestas armonizadas con vistas a encontrar soluciones comunes a los problemas planteados. Se tratará naturalmente de propuestas normativas, que pueden contribuir a corregir las múltiples deficiencias que presenta el Convenio.

[153] Art. 115.
[154] Su estructura, funcionamiento y competencias son muy similares a las que en el ámbito del Derecho comunitario se atribuyen, al denominado Grupo de Protección de las Personas frente al Tratamiento de Datos Personales. Vid. sobre ello: Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales..., cit., concretamente sus arts. 29 y 30.
[155] Art. 106.3

La composición de esta autoridad está limitada a los representantes de las autoridades nacionales de control. Cada Estado designará 2 representantes, pero sólo dispondrá de un voto deliberativo.

La conclusión de sus estudios y propuestas se harán mediante informes, que deberán ser transmitidos a las autoridades de control nacionales, así como a todos los organismos a los cuales las autoridades nacionales remiten sus propios informes. Como nada se indica, abogamos por que al menos anualmente esta autoridad elaboré un informe, que debe ser publicado, acerca del funcionamiento del Sistema Informático de Schengen, poniendo de manifiesto todas las actividades desarrolladas, los problemas suscitados, así como la actitud y cumplimiento de las garantías por parte de los Estados Miembros.

3.5. *Seguridad de los Datos.*

La seguridad de la información (protección de datos conservados, tratados y transmitidos electrónicamente) contra todo tipo de amenazas es esencial para el ejercicio efectivo de los derechos de las personas en lo referente al tratamiento automatizado de datos personales. La seguridad constituye un requisito imprescindible para la protección de personas y bienes que hacen necesarios el desarrollo de una política común tanto en el campo normativo como en el tecnológico [156].

Los peligros que amenazan a los derechos del interesado no provienen tan sólo del responsable del tratamiento. Los derechos está también amenazado si los datos los utiliza con fines diferentes un tercero que no esté autorizado a acceder a ellos ni a utilizarlos.

Es por ello que se obliga a los Estados miembros a tomar las medidas técnicas y organizativas apropiadas y necesarias para la protección contra la destrucción accidental o ilícita, contra la perdida accidental, así como contra la alteración, la comunicación y cualquier otro tratamiento no autorizado de datos personales.

Esta obligación general de seguridad se concreta en el Convenio [157] en una pormenorizada enumeración de medidas técnicas y de gestión que deberán llevarse a efecto [158].

[156] Cfr. SANCHEZ BRAVO, A., "El Tratamiento Automatizado de las Bases de Datos en el marco de la Comunidad Económica Europea: Su Protección", en Actas del III Congreso Iberoamericano de Informática y Derecho (Volumen I), Revista Informática y Derecho, Vol. 4, UNED. Centro Regional de Extremadura, Mérida, 1994.

[157] Art. 118.

[158] Dichas medidas deberán ser adoptadas por Francia, en su calidad de Parte Contratante responsable de la Unidad de Apoyo Técnico, y respecto a esta unidad.

Dichas medidas pueden agruparse atendiendo a cuatro criterios fundamentales:

— Controles personales: Para el tratamiento de datos personales sólo podrá designarse a personas especialmente cualificadas y que estén sometidas a controles de seguridad. Estas personas autorizadas sólo deben disponer de acceso a los datos que sean de su competencia (control de acceso). Estas medidas tiende a impedir que los sistemas de tratamiento de datos puedan ser utilizados por personas no autorizadas haciendo uso de las instalaciones de transmisión de datos (control de la utilización).
— Control de Instalaciones: Deben adoptarse medidas para impedir que personas no autorizadas accedan a las instalaciones utilizadas para la transmisión de datos (control de acceso a las instalaciones). Se pretende con ello salvaguardar también la integridad de los soportes de datos, y evitar que cualquier persona no autorizada, una vez que haya accedido a las instalaciones pueda leer, copiar, modificar o retirar los soportes de datos (control de los soportes de datos). Dichas medidas deben extenderse a las situaciones en que se produzca un transporte de los soportes de datos (control del transporte).
— Controles en el tratamiento: Las medidas deben tender a impedir la introducción, información, comunicación o retirada de datos sin autorización (control de la introducción de los datos). Asimismo debe poder comprobarse y verificarse posteriormente al tratamiento que datos han sido introducidos, por qué personas y en qué momentos (control de verificación de la introducción de datos).
— Controles en la transmisión: Tendrá que impedirse que los datos sean leídos, copiados, modificados o suprimidos sin autorización durante la transmisión de los datos. Deberá establecerse la posibilidad de verificar y comprobar a que autoridades se remiten datos de carácter personal a través de instalaciones de transmisión de datos[159].

Las medidas de seguridad deberán reforzarse especialmente cuando la transmisión de datos se efectué a servicios situados fuera del territorio de las Partes Contratantes. Las medidas adoptadas se comunicarán a la autoridad de control.

[159] Se recoge la obligación para los Estados miembros de dejar constancia de la transmisión y recepción de las informaciones intercambiadas, cuando de datos referentes a solicitudes de asilo (Art. 38.8) o de datos personales transmitidos en aplicación del Convenio (Art. 126.3.e) se trate.

Cuando se transmitan datos procedentes de un fichero no automatizado que se introduzcan en otro fichero no automatizado, la transmisión y recepción de datos de carácter personal quedará registrada por escrito (Art. 127.2.a).

A MODO DE CONCLUSIÓN

ALGUNAS REFLEXIONES DESDE LA FILOSOFÍA DEL DERECHO

A lo largo del nuestra exposición hemos intentado dar respuesta a las primigenias cuestiones planteadas; e incluso, a la pregunta que nos asaltaba respecto a una correcta organización expositiva y temática.

En el texto han sido ya vertidas múltiples consideraciones, disidencias, apoyos y discrepancias. Opiniones, en definitiva, nuestras, y que sometemos a la consideración y juicio del lector.

Pese a todo creo conveniente puntualizar aquellos aspectos más relevantes o polémicos; exponer la respuesta obtenida a nuestras iniciales dudas. Siguiendo nuestra exposición (1. determinación del estatuto del derecho a la libertad informática, y 2. protección de los datos personales en el ámbito de la Unión Europea), pasemos a señalar aquellos aspectos nos han llenado de racional esperanza y aquellos otros que nos han producido una honda decepción e inquietud.

I

La salvaguarda de los derechos fundamentales en esta sociedad tecnológica que nos ha tocado vivir no se concebiría de una manera racional si no otorgáramos a los ciudadanos unos mecanismos de protección adecuados a los nuevos tiempos. Es por ello que, constatada que es la información el símbolo emblemático de la nueva era, fuera necesario una adecuada ordenación de la utilización de informaciones personales, sometidas ahora a procesos informatizados de tratamiento.

Y es ahí donde se halla el origen de múltiples conflictos. Parece consolidarse en los Estados modernos una situación en la que el uso múltiple e indiscriminado de datos personales se ve como una cuestión, no solamente necesaria, sino también como algo natural. La prestación o suministro de cualquier servicio, tanto público como privado, lleva aparejada la imposición de suministrar todo una serie de datos que, en la mayoría de los casos, nada tienen que ver y son irrelevantes para la prestación del servicio de que se trate. Se crean así ingentes archivos de datos

personales, incluso de los considerados sensibles, que a la postre no están sirviendo más que como "fuentes de aprovisionamiento" para toda una legión de "indiscretos" operadores económicos.

Además, sobre todo a nivel estatal, se enarbola la eficacia en la gestión de los servicios públicos como argumento inexcusable para compeler a los ciudadanos a suministrar datos de toda naturaleza. Se pretende con ello hacer recaer sobre nosotros el sentimiento de culpabilidad por nuestra insolidaridad, si no aportamos informaciones consideradas "indispensables" para el buen funcionamiento de la "cosa pública".

Pero la culpa no es sólo de esos importantes y "potentes" sectores estatales o privados, sino que es la propia sociedad la que reclama constantemente informaciones. Pero no sobre aspectos que puedan facilitar su integración o participación personal y social. Lo que quieren saber son datos íntimos sobre la vida, fortuna o aptitudes de determinadas personas, que son considerados como referentes sociales. Las posibilidades de interconexión y entrecruzamiento de ficheros aportadas por las modernas tecnologías informáticas constituyen una inestimable ayuda para esa misión. Las denominadas "revistas del corazón" saben mucho a este respecto.

Ante estas situaciones resulta necesaria una intervención coherente que, conciliando, las necesidades sociales de información, sea respetuosa con los derechos de los ciudadanos.

El reconocimiento del derecho a la libertad informática debe constituir el eje en torno al cual se articule esa intervención.

Saliendo del estricto marco del derecho a la intimidad, el derecho a la libertad informática se configura como una exigencia ineludible para los ciudadanos de las sociedades tecnológicas. Y es que, las relaciones entre la ciencia y los derechos fundamentales no se agotan en la defensa de una parcela privada, ajena a las intromisiones de los demás, sino que se que se resuelve principalmente en un problema de libertad y dignidad.

Por que son nuestra libertad y nuestra dignidad como personas las que hoy están siendo cuestionados y menoscabados, en ara de una, no se sabe bien, "necesaria evolución tecnológica". Desgraciadamente en todo este proceso se obvia la componente humana; se avanza tan rápido que lo que menos importa son los valores personales.

De ahí que el derecho a la libertad informática sea una garantía indispensable, fruto de los nuevos retos a que se ve sometido el hombre en su libertad y dignidad. Su naturaleza peculiar y su propia esencia hacen de él un derecho típico de la tercera generación, en la línea de nuestra apuesta por una visión histórica y

generacional de los derechos fundamentales, que configura un *status* personal del ciudadano en lo referente a las informaciones que le conciernen, y que encuentra en el *status* de *habeas data* una de sus principales garantías procesales.

La toma de conciencia, en la mayor parte de los países democráticos desarrollados, acerca de la necesaria protección de los datos personales, ha llevado a la inclusión en sus legislaciones de normas sectoriales tendentes a establecer el marco en el cual podrá procederse al tratamiento de datos personales, y las garantías que para el ciudadano deben acompañar ese proceso.

Aunque con evidentes diferencias, todas las legislaciones coinciden en articular la defensa de los derechos de los ciudadanos en esta materia sobre una doble base:

1. El estricto cumplimiento del principio de "calidad de los datos" en todos los procesos de tratamiento automatizado de datos.
2. El reconocimiento de todo un elenco de derechos a favor de los particulares, que como facultades integrantes de su derecho a la libertad informática, tienden a asegurar la disponibilidad sobre los datos personales en todo el ciclo operativo de su tratamiento.

Ahora bien, y ahí que señalarlo con manifiesto desánimo, este reconocimiento legislativo, e incluso constitucional, no ha bastado *per se* para asegurar un efectivo respeto de este derecho. Su eficacia, e incluso su propia existencia, se ven cuestionadas y sometidas a constantes críticas e interesadas interpretaciones. Las limitaciones a que se ve sometido su ejercicio, por motivos en ocasiones ciertamente peregrinos, no son más que una manifestación más del intento de dejar a un lado los derechos fundamentales, cuando de intereses económicos, políticos o estratégicos estamos hablando.

Pero estas reticencias no sólo proceden de sectores "interesados". Así, una parte de la doctrina científica sigue hoy cuestionando la vigencia, e incluso la propia existencia autónoma, del derecho a la libertad informática.

Tras ello se esconde, en muchos casos, una visión inmovilista del Derecho, considerándolo como un sistema cerrado, perfecto en sí mismo, y capaz de resolver todos los problemas que se planteen a los hombres. Negando la posibilidad evolutiva del ordenamiento jurídico y de los derechos fundamentales, niegan asimismo las posibilidades evolutivas del hombre hacia mayores cotas de libertad, igualdad y solidaridad. Además, no son conscientes de que los nuevos problemas, no pueden resolverse con una adaptación, más o menos amplia, de las tradicionales estructuras jurídicas, si no que es conveniente establecer nuevos mecanismos de defensa y garantía de los derechos fundamentales acordes con los apremios de los nuevos tiempos.

Junto a esta opción doctrinal, a nuestro modesto criterio incorrecta, la defensa de unas limitaciones al derecho a la libertad informática presentan también otros frentes argumentativos:

— Para el Estado, razones de seguridad y orden público, incluso la defensa de intereses monetarios, justifica la habilitación para un tratamiento de datos personales, al margen de las garantías establecidas en las propias normas protectoras.
— Para los operadores económicos, el "correcto" funcionamiento del mercado exige un flujo tal de informaciones personales, que controlar su utilización supone un grave menoscabo para el funcionamiento de los sectores económicos, e, incluso, el propio bienestar de los ciudadanos.

Todas estas presiones han coadyuvado a que esas legislaciones de protección de datos, de cuya existencia nos congratulamos, presenten numerosas disfuncionalidades e incoherencias en su regulación: consolidación de un generoso régimen de excepciones, abuso en el empleo de conceptos jurídicos indeterminados, dependencia gubernamental de las autoridades de control, "autárquica" regulación del flujo transfronterizo de datos, etc.

De ahí que la cuestión de la protección de los datos personales no pueda considerarse, ni mucho menos, cerrada. Es necesario seguir avanzando, eliminando obstáculos y reconduciendo a sus justos términos las previsiones legislativas. No se trata de ser pesimista, como puede, y no debe, desprenderse de nuestras reflexiones. Todo lo contrario: si somos conscientes de lo que es incorrecto, podremos cambiarlo; si conocemos el mal podremos atajarlo.

Pero ello requiere que asumamos nuestras propias responsabilidades; nuestro papel en la reivindicación y defensa de nuestros derechos fundamentales. El surgimiento de una conciencia cívica, crítica e informada, puede constituir en estos días el principal motor de una reactivación en la defensa de los derechos fundamentales.

Como ha señalado Pérez Luño en una esclarecedora reflexión: *"Una sociedad libre y democrática deberá mostrarse siempre sensible y abierta a la aparición de nuevas necesidades, que fundamenten nuevos derechos. Mientras esos derechos no hayan sido reconocidos en el ordenamiento jurídico nacional y/o internacional, actuarán como categorías reivindicativas, prenormativas y axiológicas. Pero los derechos humanos no son meros postulados de deber ser. Junto a su irrenunciable dimensión utópica, que constituye uno de los polos de su significado, entrañan un proyecto emancipatorio real y concreto, que tiende a plasmarse en formas históricas de libertad, lo que conforma el otro polo de su concepto"* [1].

[1] Cfr. PEREZ LUÑO, A.E., "Intimidad y protección de datos personales: del habeas corpus al habeas data", en la obra colectiva, edic. a cargo de L. García San Miguel, Estudios sobre el derecho a la intimidad, Tecnos & Universidad de Alcalá de Henares, Madrid, 1992, pp. 36-45.

Por que, además, el Derecho no puede resolver con la celeridad y rigor que la sociedad le demanda, cuestiones que no son fruto de un día; cuestiones de un hondo calado a las que casi siempre llegará tarde.

El ordenamiento jurídico no puede estar sometido a constante revisión, ni someterse a modas más o menos pasajeras. La estabilidad que aporta a la ordenación de la vida de los pueblos no puede considerarse banalmente. Ahora bien, tampoco debe suponer un inmovilismo, ni un temor a lo desconocido. Peor que una regulación incorrecta, es aquella que olvida los destinatarios a los que va dirigida.

En definitiva, se trata de conciliar los intereses de los ciudadanos con las normas que regulan su vida y conducta; en una época, como la que nos ha tocado vivir, en la que las tensiones entre tecnología y esquemas sociales constituye uno de los signos más emblemáticos.

II

Las prevenciones apuntadas anteriormente tienen su fiel reflejo, e incluso se acrecientan, cuando nos detenemos a verificar cuál es el nivel de protección alcanzado por el derecho a la libertad informática en el ámbito comunitario.

La reciente Directiva relativa a la protección de los datos personales constituye, por ahora, el último episodio de una truculenta historia de modificaciones constantes, avances y retrocesos, alegaciones múltiples, etc., con el consiguiente riesgo para la seguridad jurídica.

Numerosas consideraciones podrían hacerse acerca de sus contenidos, previsiones o tendencias, pero creo más conveniente que ahora, llegado el momento de las últimas reflexiones, nos detengamos no tanto en sus dictados, como en su espíritu.

El enorme retraso con que en el seno de la Comunidad se aborda esta cuestión no es más que el reflejo de la falta de un verdadero interés comunitario por la materia, y de la prevalencia de los intereses económicos sobre los derechos de los ciudadanos.

Articulada su base jurídica sobre la consideración como una medida necesaria para la consecución del mercado interior, no debe extrañarnos que en la regulación de esta sensible materia, sea el criterio mercantilista el imperante, por encima de la salvaguarda de unos derechos personales, que se consideran dignos de tutela.

¿Cómo si no puede entenderse que la regulación de un derecho fundamental, se acometa dentro de las previsiones que los Tratados dedican a la consecución de determinados objetivos de convergencia económica ?

A ello hay que unir que la protección equivalente que se pretende conseguir con la puesta en marcha de la Directiva, se ve seriamente perturbada por los am-

plios márgenes de discrecionalidad que se otorga a los Estados miembros en la regulación de numerosos aspectos esenciales. Discrecionalidad que, lejos de articularse como una beneficiosa posibilidad para que los diferentes Estados miembros adapten los principios generales reguladores a las peculiaridades de su estructura jurídica, social y política, va a constituir un elemento más de distorsión, de ahondamiento en las diferencias.

En definitiva, el ideario comunitario vuelve a verse seriamente cuestionado. Los intereses nacionales, las reticencias de los Estados miembros a perder el control sobre esta importante cuestión, avalan nuestras dudas sobre la eficacia de esta regulación en curso.

No obstante sus carencias, no todo ha de ser negativo. Su articulado incorpora evidentes aciertos que es de justicia señalar. Entre otros: la eliminación de la arcaica distinción entre ficheros públicos y privados, la creación de un Grupo comunitario de contol encargado de supervisar el cumplimiento efectivo del "mandato comunitario" en las diferentes legislaciones nacionales o el establecimiento de unos controles previos para aquellos tratamientos que puedan suponer riesgos específicos para los derechos y las libertades de los interesados.

Pero si apelamos nuevamente a su espíritu, la Directiva tiene la virtualidad de un dato indiciario. La Comunidad es, al menos, consciente de la necesidad de regular la cuestiones afectantes al tratamiento y flujo de datos personales. Aún con notables deficiencias, constituye el marco jurídico regulador de los datos personales a nivel comunitario, señalando por vez primera el terreno por el que vamos a caminar. Superar sus carencias y contradicciones debe constituir la primera prueba de su consideración jurídica, y tarea inaplazable para lograr su verdadera eficacia práctica en la defensa de los derechos y libertades de los ciudadanos comunitarios.

Con respecto a los Acuerdos de Schengen, no podemos detenernos solamente a analizar la cuestión de como se arbitran mecanismos de garantía frente al uso de datos personales y su interconexión a través del "gran ordenador de Estrasburgo".

Un correcto planteamiento exige cuestionarse cuales son sus orígenes, y como éstos determinan las resultados que incorporan. Cuestiones como las relativas a los extranjeros, al problema de las fronteras - conectados ambos con la libertad comunitaria de circulación de personas -, a la cooperación en los ámbitos de la Justicia y de los asuntos de Interior no se han tratado en el seno de las instituciones comunitarias. Se ha preferido la formula de la cooperación intergubernamental para regular aspectos tan sensibles, y conseguir así un doble objetivo:

1. Evitar el debate público sobre una cuestión de vital importancia para la nueva Europa que a bombo y platillo se anuncia como " Europa de los ciudadanos ". Ciudadanos que paradójicamente aún no conocen cuales son los derechos humanos que les corresponden en cuanto tales. Ese acallar a la opinión pública, ese secretismo ha permitido que los Estados hayan desarrollado políticas ciertamente lesivas, que sólo han salido a la luz cuando estaban plenamente consolidadas y ya no cabía ningún paso atrás.

2. Obviar las medidas de control què impone el Derecho comunitario, y que son fundamentalmente el control político ejercido por el Parlamento Europeo, y el control jurisdiccional que, en su caso, correspondería al Tribunal de Justicia de las Comunidades Europeas. Como sabemos la Comunidad Europea pretende responder en su estructura organizativa a un modelo más o menos próximo al de separación de poderes. Ello implica que deben articularse una serie de garantías, entre la que destaca la publicidad y motivación de las actuaciones desarrolladas por las instituciones comunitarias. Ello supone un conocimiento por parte de los ciudadanos de las decisiones que les afectan; y les permitirá, en su caso, accionar contra las mismas cuando consideren que son lesivas para sus derechos. No podía ser de otro modo en una comunidad, que como la ha calificado el propio Tribunal de Justicia de las Comunidades Europeas, es una " Comunidad de Derecho ". Se rompe así con esa idea de " separación de poderes ", que constituyó desde sus orígenes el marco institucional de la acción comunitaria, y al que nos hemos referido anteriormente.

Estas actitudes han llevado al Parlamento Europeo, que se ha erigido en la única voz que se ha alzado para luchar contra este proceder, a denunciar el *"déficit democrático"* de esas actuaciones y a solicitar a las demás instituciones comunitarias que todas las decisiones adoptadas sobre la inmigración y la seguridad interior se traten de la misma manera que cualquier otra política comunitaria, en el marco comunitario, y no solamente entre gobiernos, para asegurar así un *"control democrático indispensable"*.

Ese proceder interestatal que venimos denunciando se ha concretado en una serie de acuerdos, convenciones y convenios, a los que nos hemos referido a lo largo de nuestra exposición. Textos que en su contenido responden a unos mismos objetivos: la defensa del orden y la seguridad públicas de los Estados miembros y, como presupuesto de lo anterior, un control efectivo sobre las fronteras exteriores de la Comunidad.

La efectividad de los controles requería un gran cantidad de información que permitiera conocer todos los aspectos, personales y materiales, que confluyeran en una determinada situación. Y es la informática la única que podía hacer frente a tales necesidades, por su facilidad y maniobrabilidad en el almacenamiento y transmisión de forma automatizada de los datos.

Todos los textos confluyen en esta necesidad, y giran sus propuestas en torno a la funcionalidad de diferentes sistemas informáticos, que aparecen como la " quinta esencia " para la solución de los problemas.Se observa una frenética activi-

dad de creación de ficheros, bancos de datos y redes informáticas, que aseguren esa puesta en marcha del control que se pretende conseguir.

Y como tal objetivo hay que decir que lo han conseguido. Pero lo han conseguido a costa de la vulneración de uno de los derechos fundamentales de todo individuo, el derecho a la intimidad.

La consolidación de una Europa policial requiere que todos estemos sometidos a un estrecho control, que casi todo lo que afecta a nuestra vida pueda ser conocido para prevenir "riesgos". Nos convertimos así en sujetos dóciles y pasivos de una vigilancia, a la que se reviste con la idea de ser necesaria para la defensa de nuestras propias identidades.

El acopio masivo de datos, y su interconexión, permite que se conozca un perfil casi exacto de nuestras vidas y actividades. Se vulnera nuestro " derecho al olvido", a que no se nos pase factura *ab aeternum* por situaciones puntuales, que no constituyen un auténtico referente de nuestra personalidad. Pero como alguien ha señalado: la mente olvida, el ordenador no.

Es en esta reflexión donde debe centrarse el énfasis de nuestras críticas. La idea de seguridad no debe en ningún caso superponerse al reconocimiento y ejercicio de nuestros derechos fundamentales. La salvaguarda de los intereses de los Estados no puede hacerse a costa de los ciudadanos.

La seguridad es fácilmente obtenible en regímenes autoritarios, donde el ciudadano es mero sufridor de la política estatal. En las sociedades democráticas, por el contrario, la seguridad es plenamente conciliable con el libre desarrollo de la personalidad y el respeto por los derechos fundamentales de los ciudadanos.

Como señaló la propia Comisión Europea allá por 1987, al presentar los objetivos primordiales de su Programa de Trabajo:

> *" Traducir Europa en hechos no se reduce únicamente a crear un espacio sin fronteras, sino que se trata asimismo de que los ciudadanos palpen Europa de forma concreta, en su vida cotidiana, en las cosas que les atañen más de cerca, a ellos y a la sociedad de nuestro tiempo, en sus intereses más inmediatos como seres humanos".*

BIBLIOGRAFÍA

APORTACIONES DOCTRINALES

ALAUX, J.P., "En Europe: "securité" d´abord, en *Le Monde Diplomatique*, juillet 1993, PP. 38-40.

ALONSO GARCIA, R., *Derecho Comunitario, Derechos nacionales y Derecho Común Europeo*, Civitas, Madrid, 1989.

ALONSO GARCIA, R., "Derechos Fundamentales y Comunidades Europeas", en la obra colectiva *Estudios sobre la Constitución Española. Homenaje al Prof. Eduardo García de Enterría*, Tomo II, Civitas, Madrid, 1991, PP. 799-836.

ALVAREZ-CIENFUEGOS SUAREZ, J.M., "La transferencia electrónica de información en la Comunidad Económica Europea", en *Actualidad Jurídica Aranzadi*, año II, núm. 37, 23 de Enero de 1992, pp. 1-2.

"Affaire Leander. Arrêt de 26 de marzo de 1987", en *Anuario de la Convención Europea de los Derechos del Hombre*, 1987.

ANCEL, P., "La protection des données personnelles. Aspects de Droit Privé français", en *Revue Internationale de Droit Comparé*, nº 3, juillet-septembre 1987, pp. 609-626.

ARA PINILLA, I., *Las transformaciones de los derechos humanos*, Tecnos, Madrid, 1990.

ARCOS VARGAS, M.C., y RODRIGUEZ BENOT, A., "La libre circulación de personas en la Unión Europea: el cruce de sus fronteras exteriores", en *Cuadernos Europeos de Deusto*, núm. 11, 1994, pp. 11-54.

ATIENZA, M., *Introducción al Derecho*, Barcanova, Barcelona, 1985.

ATIENZA, M. y RUIZ MANERO, J., "A propósito del concepto de derechos humanos de Francisco Laporta", en *Doxa*, núm. 4, 1987, pp. 67-69.

AUDIJE PACHECO, F.J.; CAMPUZANO ROBLEDO, C.; FERNANDEZ MIGUELES, D.C.; Y RUBIO SIERRA, F.J., "Consideraciones acerca de una futura ley española para limitar el uso de la informática", en *Actas del III Encuentro sobre la Informática en las Facultades de Derecho*, ICADE, Madrid, 1990, pp. 209-223.

BASAVE FERNANDEZ DEL VALLE, A., *Filosofía del Derecho Internacional*, Instituto de Investigaciones Jurídicas, UNAM, México D.F., 1985.

BEAUVERD, P., "Quelques aspects de la protection des donnees personnelles dans l´Assurance Sociale", en la obra colectiva *La protection de la personalité. Bilan et perspectives d´un nouveau droit*, Editions Universitaires Fribourg Suisse, Fribourg, 1993, pp. 87-100.

BELLUCCI, S., *SCHENGEN. L´avvio di un´Europa senza frontiere*. Edizioni Laurus Robuffo, Roma, 1995.

BERMEJO VERA, J., "Premisas Jurídicas de la intimidad personal y de la protección de los datos en el Derecho Español", en *Libro Homenaje al Profesor José Luís Villar Palasí*, Civitas, Madrid, 1989, pp. 143-161.

BOIX REIG, J., "Protección jurídico-penal de la intimidad e informática", en *Revista Poder Judicial*, nº especial IX (Nuevas formas de delincuencia), Consejo General del Poder Judicial, Madrid, 1990, pp. 17-38.
BORRAS, A., "Los ciudadanos no europeos en la Unión Europea", en *Sistema*, 114-115/1993, pp. 223-234.
BRINKSHORST, L.J., *Líneas Básicas del Derecho Europeo*, Editorial Praxis, Barcelona, 1986.
BUQUICCHIO, G., "Informática y Libertades. Balance de quince años de actividad del Consejo de Europa", trad. cast. de Isabel Hernando, en la obra colectiva *Jornadas Internacionales sobre Informática y Administración Pública*, Instituto Vasco de Administración Pública, Oñati, 1986, pp. 95-170.

CARRASCOSA GONZALEZ, J., "Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho Internacional Privado", en *Revista Española de Derecho Internacional*, vol. XLIV, núm. 2, 1992, pp. 417-441.
CARRASCOSA LOPEZ, V., "II Congreso Iberoamericano de Informática y Derecho", en *Revista Universitaria de Derecho Procesal*, 1991, núm. 5, pp. 409-414.
CARRASCOSA LOPEZ, V., "Derecho a la intimidad e informática", en *Informática y Derecho*, núm. 1, 1992, pp. 7-25.
CARRILLO SALCEDO, J.A., *Soberanía de los Estados y derechos humanos en Derecho Internacional contemporáneo*, Tecnos, Madrid, 1995.
CASADO RAIGON, R., "La actualidad de los Derechos Humanos en la Comunidad Europea y la pendiente adhesión al Convenio Europeo de 1950", en *Actas de las primeras Jornadas de Derecho Comunitario Europeo*, Universidad de Córdoba, Córdoba, 1992, pp. 71-99.
CASCAJO CASTRO, J.L., "El problema de la protección de los derechos humanos", en la obra colectiva, ed. a cargo de A.E. Pérez Luño, *Los derechos humanos: significación, estatuto jurídico y sistema*, Publicaciones de la Universidad de Sevilla, Sevilla, 1979, pp. 261-299.
CASCAJO CASTRO, J.L., "Tratamiento automatizado de los datos de carácter personal", en la obra colectiva *Problemas Actuales de los Derechos Fundamentales*, ed. a cargo de J.M.ª Sauca, Universidad Carlos III & Boletín Oficial del Estado, Madrid, 1994, pp. 363-376.
"Caso KLASS y otros. Sentencia de 6 de septiembre de 1978, serie A, núm. 28", en *BJC. Tribunal Europeo de Derechos Humanos 1959-1983*, Secretaría General del Congreso de los Diputados, Madrid, 1984, pp. 470-485.
CASTELLS ARTECHE, J. M., "Aproximación a la problemática de la Informática y Administración pública", en la obra colectiva *Jornadas Internacionales sobre Informática y Administración Pública*, Instituto Vasco de Administración Pública, Oñati, 1986, pp. 23-53.
CASTELLS ARTECHE, J. M., "La limitación informática", en la obra colectiva *Estudios sobre la Constitución Española. Homenaje al Prof. Eduardo García de Enterría*, Civitas, Madrid, 1991, pp. 907-941.
CASTRO-RIAL GARRONE, F., "Decisiones del Tribunal Europeo de Derechos Humanos (1991-1992), en *Revista de Instituciones Europeas*, vol.19, 1992, núm 2 mayo-agosto.
COHEN-JONATHAN, G., "Liberté d´expression et messsage publicitaire", en *Revue Trimestrielle des droits de l´homme*, 4 année, nº 13, janvier 1993, pp. 69-93.
COMELLA DORDA, R., "Lucas Murillo, Pablo: El derecho a la autodeterminación informativa, Tecnos, Madrid, 1990, 207 págs.", en *Revista Española de Derecho Administrativo*, 1991(72), pp. 605-610.
"Conclusiones de las Primeras Jornadas de Abogacía e Informática (Colegio de Abogados de Barcelona, 7-8 de mayo de 1993)", en *Rev. Món Jurid, Quaderns del Món Juridic*, nº 112/113,julio/agosto/ septiembre 1993, pp. I-VIII.
CONDON, R., *Computadoras*, Instituto Parramón Ediciones, Barcelona, 1982.

CHOCHEYRAS, L., "La Convention d´application de l´Accord de Schengen", en *Annuaire Français de Drit International*, Vol. XXXVII, 1991, pp. 807-818.
CHUECA SANCHO, A.G., *Los derechos fundamentales en la Comunidad Europea*, Bosch, Barcelona, 1989.

DAVARA RODRIGUEZ, M.A., "La ley española de protección de datos (LORTAD): ¿ una limitación del uso de la informática para garantizar la intimidad ? (I)", en *Actualidad Jurídica Aranzadi*, año II, núm. 76, 12 de noviembre de 1992, pp.1-5.
DAVARA DODRIGUEZ, M.A., "La ley española de protección de datos (LORTAD): ¿ una limitación del uso de la informática para garantizar la intimidad ? (II)", en *Actualidad Jurídica Aranzadi*, año II, núm. 77, 19 de noviembre de 1992, pp. 1-4.
DAVARA RODRIGUEZ, M.A., *Derecho Informático*, Aranzadi, Pamplona, 1993.
DE CASTRO CID, B., "Dimensión científica de los derechos del hombre", en la obra colectiva, ed. a cargo de A.E. Pérez Luño, *Los derechos humanos: significación, estatuto jurídico y sistema* (Actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986), Publicaciones de la Universidad de Sevilla, Sevilla, 1979, pp. 47-151.
DE LARY, H., *La libre circulation des personnes dans la CEE*, 1ª edit., Presses Universitaires de France, Paris, 1992.
DE LUCAS, J., *Europa: ¿ Convivir con la diferencia ?*, Tecnos & Fundación Enrique Luño Peña, Madrid, 1992.
DE LUCAS, J., *El concepto de solidaridad*, Fontamara, México, 1993.
DE LUCAS, J., *El desafío de las fronteras*, Ediciones Temas de Hoy, Madrid, 1994.
DE MIGUEL ZARAGOZA, J., Y BLANCO DE CASTRO, A., " El Título VI del Tratado de la Unión: Cooperación en asuntos de Justicia e Interior", *Gaceta Jurídica de la CEE y de la Competencia*, núm GJ 125, serie D, num. D-18, septiembre 1992, pp. 173-223.
DE MIGUEL ZARAGOZA, J., "La cooperación judicial en los Pactos de Schengen", *Boletín de Información del Ministerio de Justicia*, suplemento al núm. 1676, 5 de julio de 1993, pp. 3427-3441.
DEL PESO NAVARRO, E. Y RAMOS GONZALEZ, M.A., *Confidencialidad y seguridad de la información: La LORTAD y sus implicaciones socioeconómicas* , Díaz de Santos, Madrid, 1994.
DENNINGER, E., "El derecho a la autodeterminación informativa", en la obra colectiva *Problemas actuales de la Documentación y la Informática Jurídica*, ed. a cargo de A.E. Pérez Luño, Tecnos, Madrid, 1987, pp. 268-276.
DIARIO 16 ANDALUCIA, "El nuevo banco de datos policiales de Interior es ilegal, según varios comisarios", martes 2 de noviembre de 1993, pp. 16-17
DIARIO 16 ANDALUCIA, "Queja de la Defensor del Pueblo contra el GATI, nuevo banco de datos policial", sábado 13 de noviembre de 1993, p. 17.
DIEZ PICAZO, L.M., "Cambio social y evolución jurídica en la sociedad de la información", en la obra colectiva *Implicaciones socio-jurídicas de las Tecnologías de la Información*, CITEMA, Madrid, 1991, pp. 39-52.
DIEZ PICAZO, L.M., "¿ Una Constitución sin declaración de derechos ? (Reflexiones constitucionales sobre los derechos fundamentales en la Comunidad Europea)", en *Revista Española de Derecho Constitucional*, núm. 11, mayo-agosto 1991, pp. 135-155.
DIEZ PICAZO, L.M., "Reflexiones sobre la idea de Constitución Europea", en *Revista de Instituciones Europeas*, vol. 20, núm. 2, mayo-agosto 1993, pp. 533-559.
DORREGO DE CARLOS, A., "La libertad de circulación de personas: del Tratado de Roma al Tratado de la Unión Europea", en la obra colectiva *Los derechos del europeo*, ed. a cargo de J.M. Gil-Robles, Incipit Editores, Madrid, 1993, pp. 11-37.
DUBOIS, L., Y GUEYDAN, C., *Grands textes de Droit Communautaire*, 2ª edic., Dalloz, Paris, 1990.

DUPARC, C., *La Comunidad Europea y los derechos humanos*, Oficina de Publicaciones Oficiales de las Comunidades Europeas, Luxemburgo, 1993.

ESCOBAR HERNANDEZ, C., "El Convenio de aplicación del Acuerdo de Schengen y el Convenio de Dublin: una aproximación al asilo desde las perspectiva comunitaria", en *Revista de Instituciones Europeas*, vol. 20, núm 1, 1993, pp. 53-98.

ESPINAR VICENTE, J.M.: "La primacía del derecho a la información sobre la intimidad y el honor", en la obra colectiva *Estudios sobre el Derecho a la Intimidad*, Tecnos & Universidad de Alcalá de Henares, Madrid, 1992, pp. 47-67.

ESTADELLA YUSTE, O., *La protección de la intimidad frente a la transmisión internacional de datos personales*, Tecnos & Generalitat de Catalunya. Centre d´Investigació de la Comunicació, Madrid, 1995.

EUGENIO DIAZ, F., "Informatización del Derecho", en *Actas del III Encuentro sobre la Informática en las Facultades de Derecho*, ICADE, Madrid, 1990, pp. 165-183.

FERNANDEZ SANCHEZ, P.A., "La circulación de los ciudadanos extracomunitarios en la Unión Europea", en *Cuadernos Europeos de Deusto*, núm. 12, 1995, pp. 11-29.

FLUJO INTERNACIONAL DE DATOS. Recomendación de la O.C.D.E. de 23 de septiembre de 1980, Documentación Informática, Serie Amarilla. Tratados Internacionales nº 2, Presidencia del Gobierno, Madrid, 1983.

FOCSANEANU, L., "La protection des données à caractère personnel contre l´utilisation abusive de l´informatique", en *Journal du Droit International*, núm. 1, 1982, pp. 55-98.

FROSINI, V., *Cibernética, Derecho y Sociedad*, trad. cast. de C.A. Salguero-Talavera y R.L. Soriano Díaz, y Prólogo de A.E. Pérez Luño, Tecnos, Madrid, 1982.

FROSINI, V., "Banco de datos y tutela de la persona", en *Revista de Estudios Políticos*, núm. 30, noviembre-diciembre 1982, pp. 21-40.

FROSINI, V., "Los derechos humanos en la sociedad tecnológica", en *Anuario de Derechos Humanos*, núm. 2, marzo 1983, pp. 103-115.

FROSINI, V., "De la Informática Jurídica al Derecho Informático", en *Informática e Diritto*, 1983, nº 2, pp. 43-51.

FROSINI, V., "Problemas jurídicos de la Información y la Documentación", en la obra colectiva *Problemas actuales de la Documentación y la Informática Jurídica*, ed. a cargo de A.E. Pérez Luño, Tecnos, Madrid, 1987, pp. 49-52.

FROSINI, V., "Las implicaciones sociales de la revolución informática: sus ventajas e inconvenientes", en *Tecnolegis*, núm. 2, enero 1990, pp. 3-11.

FROSINI, V., "Perspectiva: De la Informática jurídica al Derecho de la Informática", en *Tecnolegis*, núm. 11, abril-junio 1992, pp. 3-11.

FROSINI, V., "L´organizzazione informatica dello stato e la libertà del cittadino", en *Il Diritto dell´informazione e dell´informatica*, anno IX, nº 3, maggio-giugno 1993, pp. 599-608.

FROSINI, V., "Por una Sociología de los derechos humanos en la era tecnológica", trad. cast. de Carlos Alarcón Cabrera, en *Derechos y Libertades. Revista del Instituto Bartolomé de las Casas*, año I, octubre 1993 - marzo 1994, núm. 2, pp. 201-210.

GALINDO AYUDA, F., "Consecuencias de la entrada de España en la Comunidad Económica Europea en el derecho español de la informática", en la obra colectiva *Derecho español y Derecho Comunitario Europeo*, Servicio de Publicaciones de la Universidad de Zaragoza, Zaragoza, 1987, pp. 389-426.

GARCIA CAMARERO, E., "Bases de Datos y representación del conocimiento", en *Theoría*, año I (1985), nº 1, pp. 293-303.

GARCIA GALAN, J.L., "La libre circulación de personas en el Espacio Schengen, una realidad desde 1995", en Rev. *Europa Junta*, núm. 37, abril 1995, pp. 5-15.

GARCIA-PABLOS MOLINA, A., "Informática y Derecho Penal", en la obra colectiva *Implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, Madrid, 1991, pp. 61-71.

GARCIA RODRIGUEZ, I., "Derecho aplicable y orden público comunitario", en *Revista de Instituciones Europeas*, vol. 20, nº 3, septiembre-diciembre 1993, pp. 927-941.

GARCIA SAN MIGUEL RODRIGUEZ-ARANGO, L. (edic. a cargo de), "Reflexiones sobre la intimidad como límite de la libertad de expresión", en la obra colectiva *Estudios sobre el Derecho a la Intimidad*, Tecnos & Universidad de Alcalá de Henares, Madrid, 1992, pp. 15-35.

GARZON CLARIANA, G., "La protección de los datos personales y la función normativa del Consejo de Europa", en *Revista de Instituciones Europeas*, vol. 8, enero-abril 1981, pp. 9-25.

GARZON CLARIANA, G., "La protección jurídica de los datos de carácter personal", en la obra colectiva *Implicaciones socio-jurídicas de las Tecnologías de la Información*, CITEMA, Madrid, 1991, pp. 21-32.

GAUTIER, Y., "La coopération policière: les perspectives ouvertes par le traité sur l´Union Européenne du 7 février 1992", en *EUROPE*, 3 année, nº 4, avril 1993, pp. 1-5.

GAUTIER, Y., "Les Accords de Schengen et le droit d´asile à l´épreuve du débat constitutionel", en *EUROPE*, 3 année, nº 12, décembre 1993, pp. 1-3.

GOMEZ TORRES, C.J., "El abuso de los derechos fundamentales", en la obra colectiva, ed. a cargo de A.E. Pérez Luño, *Los derechos humanos: significación, estatuto jurídico y sistema*, Publicaciones de la Universidad de Sevilla, Sevilla, 1979, pp. 301-332.

GONZALEZ-TABLAS SASTRE, R., *La Informática Jurídica. Un análisis experimental desde la Filosofía del Derecho*, Sevilla, Tesis Doctoral, 1986.

GONZALEZ-TABLAS SASTRE, R., "Los nuevos problemas de los "Documentos y Datos" en soportes informáticos", en la obra colectiva *El abogado. Formación, deontología y organización del despacho profesional*, Aranzadi Editorial, Pamplona, 1994, pp. 165-171.

GREMY, F., "Protection des donnés médicales nominatives", en la obra colectiva *Informatique Médicale*, Flammarion, Paris, 1987, pp. 421-440.

GUERRERO, M.F., "Los Sistemas Jurídicos Expertos: La inteligencia artificial aplicada al Derecho", en *Actas del III Encuentro sobre la Informática en las Facultades de Derecho*, ICADE, Madrid, 1990, pp. 21-51.

HEREDERO HIGUERAS, M., "La protección de datos personales en manos de la policía: reflexiones sobre el Convenio de Schengen", en la obra colectiva *La protección de los datos personales. Regulación Internacional de la seguridad informática*, Monografies i Documents, núm. 8, Centre d´Investigació de la Comunicació i Universitat Pompeu Fabra, Generalitat de Catalunya, Barcelona, 1993, pp. 31-47.

HEREDERO HIGUERAS, M., "La Agencia de Protección de Datos", en *Informática y Derecho*, núms. 6-7, 1994, pp. 323-357.

HEREDERO HIGUERAS, M., *La Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal. Comentario y Textos*, Tecnos, Madrid, 1996.

HERNANDO, I., "La Comunidad Económica Europea y la Informática", en la obra colectiva *Jornadas Internacionales sobre Informática y Administración Pública*, Instituto Vasco de Administración Pública, Oñati, 1986, pp. 79-93.

HONDIUS, F.W., "Notas sobre el Derecho a la protección de datos", en la obra colectiva *Implicaciones socio-jurídicas de las Tecnologías de la Información*, CITEMA, Madrid, 1991, pp. 33-38.

HREBLAY, V., *La libre circulation des personnes. Les Accords de Schengen*, Presses Universitaires de France, Paris, 1991.

HUET, J., "Aspects juridiques de l´EDI, Echange de Données Informatisées (Electronic Data Interchange)„ en *Recueil Dalloz Sirey*, 1991, 27 Cahier-Chronique, pp. 181-188.
Informe de la Comisión Calcutt sobre la Intimidad y Cuestiones Afines, trad. cast. de M.A. Sánchez Suarez, Cuadernos del Consejo General del Poder Judicial, núm. 4, 1991.

JIMENEZ CAMPO, J., "La garantía constitucional de las comunicaciones", en *Revista Española de Derecho Constitucional*, múm. 20 (mayo-agosto 1987).
JONGEN, F., "La liberté d´expression dans l´audiovisuel: liberté limitée, organisée et surveillée", en *Revue Trimestrielle des Droits de l´homme*, 4 année, nº 13, janvier 1993, pp. 95-117.
JULIEN-LAFERRIERE, F., "L´Europe de Schengen: de la disparition des frontieres aux transferts des controles", en *Actualité Legislative DALLOZ*, nº 13, juillet 1992, pp. 125-130.

KAYSER, P., *La protection de la vie privée. Tome I: Protection du secret de la vie privée*, Económica, Paris, 1984.
KAYSER, P., *La protection de la vie privée*, 2º edit., Económica, Paris, 1990.
KNAPP, B., "La protection des données personnelles. Droit Public Suisse", en *Revue Internationale de Droit Comparé*, nº 3, juillet-septembre 1987, pp. 581-605.

LAPORTA, F., "Sobre el concepto de derechos humanos", en *Doxa*, núm. 4, 1987, pp. 23-46.
LAPORTA, F., "Respuesta a Pérez Luño, Atienza y Ruiz Manero", en *Doxa*, núm. 4, 1987, pp. 71-77.
LAZARO MORENO, F., *El Acuerdo de Schengen y la libre circulación de personas en la C.E.E.*, Cuadernos de Europa, nº 2, Diputación de Zaragoza (Comisión de Europa), Zaragoza, 1993.
LAZPITA GUTURBAY, M., "La protección de los datos personales en la Comunidad Europea", en *Cuadernos Europeos de Deusto*, núm. 9, 1993, pp. 41-61.
LEGAZ Y LACAMBRA, L., *Filosofía del Derecho*, 5ª Edic., Bosch, Barcelona, 1979.
LOPEZ GARRIDO, D., "Administración Parlamentaria e Informática", en la obra colectiva *Jornadas Internacionales sobre Informática y Administración*, Instituto Vasco de Administración Pública, Oñati, 1986, pp. 69-75.
LOPEZ GARRIDO, D., "La sociedad informatizada y la crisis del Estado de bienestar", en *Revista de Estudios Políticos*, núm. 48, noviembre-diciembre 1985, pp. 27-45.
LOPEZ GARRIDO, D., *Aspectos de inconstitucionalidad de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento automatizado de los datos de carácter personal*, enero, 1993. (Dictamen a solicitud de la Comisión de Libertades e Informática).
LOPEZ MAYOR, V., "La legislación española sobre Informática en el ordenamiento jurídico español", en *Actas del Congreso sobre Derecho Informático*, Facultad de Derecho de Zaragoza, Zaragoza, 1989, pp. 415-446.
LORCA NAVARRETE, J.F., *Introducción al Derecho. Fundamentos filosóficos*, Pirámide, Madrid, 1987.
LOSANO, M.G., *Los grandes sistemas jurídicos. Introducción al Derecho europeo y extranjero*, trad. cast. de A. Ruiz Miguel, Debate, Madrid, 1982.
LOSANO, M.G., *Curso de Informática Jurídica*, Tecnos, Madrid, 1987.
LUCAS MURILLO DE LA CUEVA, P., "La protección de los datos personales ante el uso de la informática", en *Anuario de Derecho Público y Estudios Políticos*, núm. 2, 1989/90, pp. 153-170.
LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa. La protección de datos personales ante el uso de la informática*, Tecnos, Madrid, 1990.
LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993.

MAISL, H., "Etat de la législation française et tendances de la jurisprudence relatives a la protection des données personnelles", en *Revue Internationale de Droit Comparé*, nº 3, juillet-septembre 1987, pp. 559-580.
MADRID CONESA, F., *Derecho a la intimidad, informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984.
MARTINEZ DE PISON CAVERO, J., *El derecho a la intimidad en la jurisprudencia constitucional*, Civitas, Madrid, 1993.
MASSE, M., "L´espace Schengen.I.- Textes et contexte, figures de l´integration dans l´Europe communautaire", en *Revue de Science Criminelle et Droit Penal comparé*, (2), avril-juin 1992, pp. 373-388.
MASSE, M., "L´Organisation Internationale de Police Criminelle (O.I.P.C.-INTERPOL), en *Revue de Science Criminelle et Droit Pénal comparé*, (2), avr-juin 1992, pp. 376-379.
MASSE, M., "L´espace Schengen.II.- Developpements de l´entraide repressive internationale", *en Revue de Science Criminelle et Droit Pénal comparé*, (4), oct-dèc 1992, pp. 800-808.
MENENDEZ, J., "Colisión del derecho a la verdad con otros derechos básicos" en la obra colectiva *Persona y Derecho*, Vol. V, 1987, pp. 50-53.
MIRABELLI, G., "In tema di tutela dei dati personali (Note a margine della proposta modificata di Direttiva CEE) en *Il diritto dell´informazione e dell´informatica*, anno IX, nº 3, maggio-giugno 1993, pp. 609-626.
MONTAVON, P., "De la confidentialite des donnes personnelles au sein des enterprises", en la obra colectiva *La protection de la personalité. Bilan et perspectives d´un nouveau droit*, Editions Universitaires Fribourg Suisse, Fribourg, 1993, pp. 75-85.
MUÑOZ MACHADO, S. y otros, *Código de Derecho Comunitario Europeo. Tratados, Derecho derivado, Jurisprudencia*, Civitas, Madrid, 1988.
MURILLO FERROL, F., "El impacto de las tecnologías y medios de información en el Derecho Político", en la obra colectiva *Implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, Madrid, 1991, pp. 115-124.

NEEL, B., "L´Europe sans frontières interieures: l´accord de Schengen", en *Actualité juridique. Droit Administratif*, 1991, núm. 10. pp. 659-679.
NORA, S. Y MINC, A., *La informatización de la sociedad*, trad. cast. de P. García de Pruneda y R. Ruza, Fondo de Cultura Económica, México-Madrid-Buenos Aires, 1980.

OLIVE, L., "Racionalidad y progreso del desarrollo científico: una controversia metametodológica", en *Theoria*, vol.VII, 1992, nº 16-17-18, tomo A, pp. 41-56.
ORTIZ Y CHICA, J.M., "ROMEO CASABONA: Poder informático y seguridad jurídica (Colección Impactos, Los Libros de Fundesco, Madrid, 1987)", en *Revista Crítica de Derecho Inmobiliario*, 1990, núm. 597, pp. 879-881.

PECES-BARBA MARTINEZ, G., *Tránsito a la modernidad y derechos fundamentales*, Mezquita, Madrid, 1982.
PEREZ LUÑO, A.E., *Cibernética, Informática y Derecho. Un análisis metodológico*, Publicaciones del Real Colegio de España, Bolonia, 1976.
PEREZ LUÑO, A.E., "Informática jurídica y Derecho de la informática en España", en *Informatica e Diritto*, 1983, nº 2, pp. 81-99.
PEREZ LUÑO, A.E., "La defensa del ciudadano y la protección de datos", en la obra colectiva *Jornadas Internacionales sobre Informática y Administración Pública*, Instituto Vasco de Administración Pública, Oñati, 1986, pp. 55-68.

PEREZ LUÑO, A.E., "La defensa del ciudadano y la protección de datos", en *Revista Vasca de Administración Pública*, núm 14 (1986), pp. 43-55.
PEREZ LUÑO, A.E., "La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo", en *Anuario de Derechos Humanos*, (4) 1986-1987, pp. 259-289.
PEREZ LUÑO, A.E., *Nuevas Tecnologías, Sociedad y Derecho. El impacto socio-jurídico de las N.T. de la información*, Fundesco, Madrid, 1987.
PEREZ LUÑO, A.E., "Introducción a los sistemas informatizados de Documentación Jurídica", en la obra colectiva *Problemas actuales de la Documentación y la Informática Jurídica*, ed. a cargo de A.E. Pérez Luño, Tecnos, Madrid, 1987, pp. 27-48.
PEREZ LUÑO, A.E., "Concepto y concepción de los derechos humanos (Acotaciones a la ponencia de Francisco Laporta)", en *Doxa*, núm. 4, 1987, pp. 47-66.
PEREZ LUÑO, A.E., *Los Derechos Fundamentales*, 3ª edic., Tecnos, Madrid, 1988.
PEREZ LUÑO, A.E., "La libertad informática. Nueva frontera de los derechos fundamentales", en la obra colectiva *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989, pp.137-162.
PEREZ LUÑO, A.E., "La incorporación del Convenio Europeo sobre protección de datos personales al ordenamiento jurídico español", en la obra colectiva *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989, pp. 163-184.
PEREZ LUÑO, A.E., "Iniciativas y proyectos de leyes españoles sobre informática y libertades", en la obra colectiva *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989, pp. 185-213.
PEREZ LUÑO, A.E., "La incorporación del Convenio europeo sobre protección de datos al ordenamiento jurídico español", en *ICADE. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales*, núm. 17, 1989. pp. 27-ss.
PEREZ LUÑO, A.E., "Nuevos derechos fundamentales de la era tecnológica: la libertad informática", en *Anuario de Derecho Público y Estudios Públicos*, núm. 2, 1989/90, pp. 171-195.
PEREZ LUÑO, A.E., "Las generaciones de derechos fundamentales", en *Revista del Centro de Estudios Constitucionales*, núm. 10, 1991, pp. 203-217.
PEREZ LUÑO, A.E., "Implicaciones socio-jurídicas de las tecnologías de la información", en la obra colectiva *Implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, Madrid, 1991, pp. 273-290.
PEREZ LUÑO, A.E., "Impacto de la informática en el sistema de valores jurídicos", en la obra colectiva *Implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, Madrid, 1991, pp. 355-365.
PEREZ LUÑO, A.E., "Informática y Derecho hoy", en la obra colectiva *Implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, Madrid, 1991, pp. 429-441.
PEREZ LUÑO, A.E., "Los derechos de la era tecnológica en la obra de Vittorio Frosini", en *Theoria*, vol. VII, 1992, nº 16-17- 18, tomo B, pp. 1101-1113.
PEREZ LUÑO, A.E., "Intimidad y protección de datos personales: Del *habeas corpus* al *habeas data*", en la obra colectiva *Estudios sobre el Derecho a la Intimidad*, Tecnos & Universidad de Alcalá de Henares, Madrid, 1992, pp. 36-45.
PEREZ LUÑO, A.E., "Del *habeas corpus* al *habeas data*", en *Informática y Derecho*, núm. 1, UNED-Mérida, 1992, pp. 153-161.
PEREZ LUÑO. A.E., *El desbordamiento de las fuentes del Derecho*, Real Academia Sevillana de Legislación y Jurisprudencia, Sevilla, 1993.
PEREZ LUÑO, A.E., "Comentario legislativo: La LORTAD y los derechos fundamentales", en *Derechos y Libertades. Revista del Instituto Bartolomé de las Casas*, 1993, febrero-octubre, nº 1, pp. 405-424.

PEREZ LUÑO, A.E., "El asalto informático a las libertades (I)", en *Diario 16 Andalucía*, lunes 18 de enero de 1993, p. 4.
PEREZ LUÑO, A.E., "El asalto informático a las libertades (II)", en *Diario 16 Andalucía*, martes 19 de enero de 1993, p. 4.
PEREZ LUÑO, A.E., "Gestión (automatizada) del despacho profesional del abogado", en la obra colectiva *El abogado. Formación, deontología y organización del despacho profesional*, Aranzadi Editorial, Pamplona, 1994, pp. 147-163.
PEREZ LUÑO, A.E., "Dilemas actuales de la protección de la intimidad", en la obra colectiva *Problemas Actuales de los Derechos Fundamentales*, ed. a cargo de J.M.ª Sauca, Universidad Carlos III & Boletín Oficial del Estado, Madrid, 1994, pp. 311-337.
PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho y Constitución*, 5ª Edic., Tecnos, Madrid, 1995.
PEREZ LUÑO, A.E., *Manual de Informática y Derecho*, Ariel, Barcelona, 1996.
"Portugal no asumirá la Presidencia de Schengen. Incumplimientos", en *ABC Sevilla*, miercoles 16 de febrero de 1994, p. 30.
POYAL COSTA, A., "La eficacia de los derechos humanos frente a terceros" en *Revista de Derecho Político*, núm. 34, 1991, pp. 189-221.

RIGAUX, F., "La loi applicableà la protection des individus à l´egard du traitement automatisé des données à caractère personnel", en *Revue Critique de Droit International Privé*, 1980, pp. 443-478.
RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, Brylant-L.G.D.J., Bruselas, 1990.
RIGAUX, F., "Introduction Générale", en la obra colectiva *La liberté d´expression, son étendue et ses limites*, en Revue Trimestrielle des Droits de l´homme, 4 année, nº 13, janvier 1993, pp. 3-22.
RIPOL CARULLA, S., "El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal: Balance a los seis años de su apertura a la firma" en *Actas del Congreso sobre Derecho Informático*, Zaragoza, 1989, pp. 395-413.
RIPOL CARULLA, S., *Las libertades de información y de comunicación en Europa*, Tecnos & Fundación Enrique Luño Peña, Madrid, 1995.
ROGGE, K., "La protection de la vie privée et les défis tecnologiques", traduction de l´anglais par Viviane François, en *Revue Trimestrelle des Droits de l´homme*, núm. 17, janvier 1994.
ROMEO CASABONA, C.M., *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las nuevas tecnologías de la información*, Fundesco, Madrid, 1988.
ROSENBAUM, J.I., "The European Comission´s Draft Directive on Data Protection", en *Jurimetrics. Journal of Law, Science and Tecnology*, vol. 33, núm. 1, 1992, pp. 1-12.
ROVIRA VIÑAS, A., "Reflexiones sobre el derecho a la intimidad en relación con la informática, la medicina y los medios de comunicación", en *Revista de Estudios Políticos*, núm. 77, julio-septiembre 1992, pp. 259-265.
RUIZ MIGUEL, C., "La tercera generación de los derechos fundamentales" (Crónica del Seminario celebrado en Cordoba, los días 8 y 9 de marzo de 1991 en la Facultad de Derecho, acerca de la tercera generación de derechos fundamentales), en *Revista de Estudios Políticos*, núm. 72, abril-junio 1991, pp. 301-312.

RUIZ MIGUEL, C., *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, Civitas, Madrid, 1994, pp. 49-54.

SANCHEZ AGESTA, L., "El impacto de las tecnologías y medios de información en el Derecho español y el Derecho comparado", en la obra colectiva *Implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, Madrid, 1991, pp. 125-130.

SANTAMARÍA PASTOR, J.A., "Sobre el derecho a la intimidad, secretos y otras cuestiones innombrables", en *Revista Española de Derecho Constitucional*, núm. 15, septiembre-diciembre 1985, pp. 159-180.

SANTAOLALLA GADEA, F.J., "La integración del Derecho de las Comunidades Europeas en el ordenamiento español: algunas zonas oscuras del *acquis* communautaire", en *Documentación Administrativa*, núm. 193, 1982, pp. 5-75.

SIMITIS, S., "Crisis de la información en el Derecho y sistemas informatizados de Documentación Jurídica", en la obra colectiva *Problemas actuales de la Documentación y la Informática Jurídica*, ed. a cargo de A.E. Pérez Luño, Madrid, 1987, pp. 53-59.

SIMITIS, S., "Datenschuntz und Europäische Gemeinschaft", en *RDV*, 1990, Heft 1, pp. 3-23.

SIMITIS, S., "From the Market to the Polis: The EU Directive on the Protection of Personal Data", en *Iowa Law Review*, vol. 80, nº 3, march 1995, pp. 445-469.

STRANGAS, J., "Las relaciones entre la Informática y los fines de la Filosofía del Derecho", trad. cast. de Carlos Alarcón, en *Informàtica y Derecho*, núm. 8, 1995, pp. 195-215.

TELLEZ VALDES, J., *Derecho Informático*, Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas, México D.F., 1987.

TESANDE CALVO, J.J., "Notas al proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal", en *Poder Judicial*, núm. 23, septiembre 1991, pp. 105-112.

TOMAS AZPILCUETA, H., *Derecho Informático*, Abeledo-Perrot, Buenos Aires, 1987.

TONIATTI, R., "Libertad informática y derecho a la protección de los datos personales: Principios de legislación comparada", trad. cast. de A. Saiz Arnaiz, en *Revista Vasca de Administración Pública*, 1991, enero-abril, nº 29, pp. 139-162.

TORNE-DOMBIDAU JIMENEZ, J. Y CASTILLO BLANCO, F.A., "Informática y protección de la privacidad del individuo (I). (a propósito de las recientes reformas legislativas establecidas por la Ley de regulación del tratamiento automatizado de los datos de carácter personal y la Ley de régimen jurídico de las administraciones públicas y del procedimiento administrativo común)", en *Actualidad Administrativa*, nº 22/31 mayo-6 junio 1993, pp. 267-277.

TORNE DOMBIDAU JIMENEZ, J. Y CASTILLO BLANCO, F.A., "Informática y protección de la privacidad del individuo (II)", en *Actualidad Administrativa*, nº 23/ 7-13 junio 1993, pp. 279-288.

TORNE-DOMBIDAU JIMENEZ, J. Y CASTILLO BLANCO, F.A., "Informática y protección de la privacidad del individuo (y III), en *Actualidad Administrativa*, nº 24/14-20 junio 1993, pp. 289-297.

TRUYOL SERRA, A., "Bases filosóficas y metodológicas para un Derecho de la sociedad de la información", en la obra colectiva *Implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, Madrid, 1991, pp. 139-143.

URIO RODRIGUEZ, R. Y DIEZ BERNAL, M.J., "Los sistemas expertos en el mundo del Derecho", en *Actas del III Encuentro sobre la Informática en las Facultades de Derecho*, ICADE, Madrid, 1990, pp. 225-232.

VEDEL, G., "Schengen et Maastrich (A propos de la décision nº 91-294 DC du Conseil constituionnel du 25 juillet 1991), en *Revue Française Droit Administratif*, 8 (2), mars-avril 1992, pp. 173-184.

VICENTE BLANCO, D.J., "El sistema de los acuerdos de Schengen desde el Derecho Internacional Privado (I). Las técnicas jurídicas utilizadas en el proceso de génesis hacia la supresión de las fronteras interiores en el ámbito comunitario (perspectiva general y de cooperación)", *Revista de Estudios Europeos*, mayo-agosto, 1995, núm. 10, pp. 47-80.

VILARIÑO PINTOS, E., "El impacto de las tecnologías y medios de información en el Derecho Internacional", en la obra colectiva *Implicaciones socio-jurídicas de las tecnologías de la información*, CITEMA, Madrid, 1991, pp. 131-137.

VILLAR PALASI, J.L., "El Derecho frente al reto informático", en *Actas del II Encuentro sobre la Informática en las Facultades de Derecho*, ICADE, Madrid, 1988.

VITALIS, A., *Informatique, Pouvoir et Libertès*, Economica, Paris, 1981.

WECKEL, P., "La Convention Additionelle a l'Accord de Schengen", en *Revue Générale de Droit Internationale Public*, Tome 95/1991/2, pp. 405-437.

DOCUMENTOS DE LAS INSTITUCIONES COMUNITARIAS

COMISION DE LAS COMUNIDADES EUROPEAS

Recomendación de la Comisión, de 29 de julio de 1981, relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, DOCE Nº L 246/31, 29.8.81.

Propuesta de Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales, COM (90) 314 final - SYN 288, 24.09.1990.

Propuesta modificada de Directiva 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, COM (92) 422 final - SYN 287, 15.10.1992.

El acceso de los ciudadanos a los documentos de las Instituciones (Comunicación al Consejo, al Parlamento Europeo y al Comité Económico y Social), DOCE Nº C 156/5, 8.6.1993.

Propuesta de Reglamento, basado en el artículo 100 C del Tratado constitutivo de la Comunidad Europea, por el que se determinan los terceros países cuyos nacionales deben estar provistos de un visado al cruzar las fronteras exteriores de los Estados miembros, COM (93) 684 final, DOCE Nº C 11/15, 15.1.94.

Propuesta de Decisión, basada en el artículo K.3 del Tratado de la Unión Europea, por la que se aprueba el Convenio sobre el paso de las fronteras exteriores de los Estados miembros, COM (93) 684 final, DOCE Nº C 11/6, 15.1.94.

Propuesta modificada de Directiva del Parlamento Europeo y del Consejo relativa a la protección de los datos personales y la intimidad en relación con las redes digitales de telecomunicación y, en particular, con la Red Digital de Servicios Integrados (RDSI) y las redes móviles digitales públicas, COM (94) 128 final/2-COD 288, 15.6.1994.

Europa en marcha hacia la sociedad de la información. Plan de actuación. Comunicación de la Comisión al Consejo y al Parlamento Europeo y al Comité Económico y Social y al Comite de Regiones, COM (94) 347 final, 19.07.1994.

Recomendación 92/820/CE de la Comisión, de 19 de octubre de 1994, relativa a los aspectos jurídicos del intercambio electrónico de datos, DOCE Nº L 338/98, 28.12.1994.

Comunicación de la Comisión al Parlamento Europeo, con arreglo al párrafo segundo del apartado 2 del artículo 189 B del Tratado CE. Posición común del Consejo aprobada el 20 de febrero de 1995 sobre la 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 y a la libre circulación de estos datos, SEC (95) 303 final - COD 287, 24.02.1995.

Propuesta de Directiva del Consejo relativa al derecho de nacionales de terceros países a viajar dentro de la Comunidad, COM (95) 346 final, 12.07.1995.

Propuesta de Directiva del Consejo relativa a la supresión de los controles sobre las personas en las fronteras interiores, COM (95) 347 final, 12.07.1995.

Dictamen de la Comisión con arreglo a la letra d) del apartado 2 del artículo 189 B del Tratado CE, sobre las enmiendas del Parlamento Europeo a la posición común del Consejo sobre la 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 y a la libre circulación de estos datos, por el que se modifica la propuesta de la Comisión con arreglo al apartado 2 del artículo 189 A del Tratado CE, COM (95) 375 final-COD287, 18.07.1995.

CONFERENCIA INTERGUBERNAMENTAL 1996. Informe de la Comisión para el Grupo de reflexión, Oficina de Publicaciones Oficiales de las Comunidades Europeas, Luxemburgo, 1994.

CONSEJO DE MINISTROS

Directiva 91/250/CEE del Consejo, de 14 de mayo de 1991, sobre protección jurídica de programas de ordenador, DOCE Nº L 122/42, 17.5.1991.

Decisión 92/242/CEE del Consejo, de 31 de marzo de 1992, relativa a la seguridad de los sistemas de información, DOCE Nº L 123/19, 8.5.1992.

Resolución del Consejo, de 20 de julio de 1994, relativa la coordinación en materia de intercambio de datos entre administraciones, DOCE Nº C 181/1, 1.7. 1994.

Acción común 95/73/JAI, de 10 de marzo de 1995, adoptada por el Conmsejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativo a la Unidad de Drogas de Europol, DOCE Nº L 62/1, 20.3.1995.

Posición Común (CE) Nº 1/95, adoptada por el Consejo el 20 de febrero de 1995, con vistas a la adopción de la Directiva 95/.../CE del Parlamento Europeo y del Consejo, de..., 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, DOCE Nº C 93/1, 13.4.1995.

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 automatizado de datos personales y a la libre circulación de estos datos, DOCE Nº L 281/31, 23.11.1995.

COMITE ECONOMICO Y SOCIAL

Dictamen sobre la propuesta de Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales, DOCE Nº C 159/38 de 17.6.1991

PARLAMENTO EUROPEO

Resolution sur la protection des droits de la personne face au développement des progrés techniques dans le domaine de l´informatique, JOCE, Nº C 140/34, 5.6.1979.

Resolution sur la protection des droits de la personne face au développement des progrés techniques dans le domaine de l´informatique, JOCE, Nº C 87/39, 5.4.1982.

Resolución por la que se aprueba la Declaración de los Derechos y Libertades Fundamentales, DOCE Nº C 120/51, 16.5.1989.

Resolución, de 23 de noviembre de 1993, sobre la firma del Acuerdo adicional de Schengen, DOCE Nº C 323/98, 27.12.1989.

Resolución, de 15 de marzo de 1990, sobre la libre circulación de las personas en el mercado interior, DOCE Nº C 96/274, 17.4.1990.

Resolución, de 14 de junio de 1990, sobre el Acuerdo de Schengen y el Convenio relativo al derecho de asilo y al estatuto de los refugiados del Grupo ad hoc sobre inmigración, DOCE Nº C 175/170, 16.7.1990.

Parlamento Europeo. Comisión de Investigación del Racismo y la Xenofobia. Informe sobre las Conclusiones, Oficina de Publicaciones Oficiales de las Comunidades Europeas, Luxemburgo, 1991.

Resolución, de 22 de febrero de 1991, sobre la armonización de las políticas de acceso a los territorios de los Estados miembros de la CE, con vistas a la libre circulación de las personas (art. 8 del Tratado CEE) y la elaboración de una convención intergubernamental entre los doce Estados miembros de la Comunidad, DOCE Nº C 72/213, 18.03.1991.

Dictamen del Parlamento Europeo sobre la propuesta de la Comisión al Consejo referente a una directiva relativa a la protección de las personas en lo referente al tratamiento de datos personales, DOCE Nº C 94/198, 13.4.1992.

Resolución sobre la entrada en vigor de los Acuerdos de Schengen, DOCE Nº C 337/214, 21.12.1992.

Parlamento Europeo. Fichas Técnicas sobre el Parlamento Europeo y las actividades de la Unión Europea, Parlamento Europeo. Dirección General de Estudios, Luxemburgo, 1994.

Recurso interpuesto el 18 de noviembre de 1993 contra la Comisión de las Comunidades Europeas por el Parlamento Europeo (Asunto C-445/93), DOCE Nº C 1/12, 4.1.1994.
Resolución sobre el Acuerdo de Schengen y la política de asilo, DOCE Nº C 109/169, 1.5.1995.

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 automatizado de datos personales y a la libre circulación de estos datos, DOCE Nº L 281/31, 23.11.1995.

Se acabó de imprimir
este libro en los talleres de
EUROPA ARTES GRÁFICAS, S.A.,
el día 8 de enero
de 1999, festividad de
San Severino