EN TORNO A LA PROTECCION DE LOS DATOS PERSONALES AUTOMATIZADOS

Por CARLOS RUIZ MIGUEL

SUMARIO

España ratificó en 1985 el Convenio 108 del Consejo de Europa de protección de datos personales (1). Se ha tardado un tiempo inusual en desarrollar la legislación nacional oportuna. Podría pensarse que si por fin se ha procedido a este desarrollo es por virtud de las exigencias impuestas en el acuerdo de Schengen. En efecto, el Acuerdo de Adhesión del Reino de España al Convenio de Schengen contiene una declaración común de las partes contratantes en cuya virtud «el Gobierno del Reino de España se obliga a adoptar, antes de la ratificación del Acuerdo de Adhesión al Convenio de 1990 (el Convenio de Schengen), todas las iniciativas necesarias para que la legislación española sea completada de conformidad con el Convenio de Europa de 28 de enero de 1981 para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal y con observancia de la Recomendación R (87) 15, de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa, tendente a reglamentar la utilización de los datos de carácter personal en el sector policial». Este compromiso se asumía para poder dar plena aplicación a las disposiciones de los artículos 117 y 126 del Convenio de Schengen, entre otros, relativos a la protección de los datos de carácter personal, y para poder llegar a un nivel de protección compatible con las disposiciones del acuerdo de Schengen (2).

(1) Convenio 108 del Consejo de Europa, de 28 de enero de 1981, sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado por España y publicado en el *Boletín Oficial del Estado* de 15 de noviembre de 1985.

(2) Declaración común concerniente a la protección de datos incluida en el Acta final del Acuerdo de Adhesión del Reino de España al Convenio de Schengen de 19 de junio de 1990. El instrumento de ratificación, el acuerdo de Adhesión del Reino de España y el texto del Convenio de Schengen han sido publicados en el *Boletín Oficial del Estado* del 5 de abril de 1994.

Dada la prácticamente absoluta falta de elementos legales y jurisprudenciales sobre este terreno, la doctrina se ha convertido en ariete para la defensa de los derechos fundamentales a través de sus aportaciones. Entre las aparecidas en estos años creo que merecen destacarse las del profesor Pablo Lucas Murillo. Su contribución consiste en dos libros: *El derecho a la autodeterminación informativa* (Madrid, Tecnos, 1990) e *Informática y protección de datos personales* (Madrid, CEC, 1993), amén de otros artículos (3). Constituyen un conjunto que se caracteriza por dos notas características: su enfoque jurídico-constitucional y su atención al ordenamiento español. Por lo demás, como afirma el autor, entre sus dos libros existe una íntima unidad, o mejor continuidad, pues el último de ellos estudia en profundidad la LORTAD (4), que no estaba promulgada cuando se elaboró el primero. La aparición de la LORTAD, la definitiva ratificación y publicación del Acuerdo de Schengen, la emisión por el TC de una importante sentencia sobre el asunto (5) y la publicación de estas obras del profesor Lucas Murillo nos invitan a considerar la cuestión de la protección de datos personales.

I. EL MARCO CONCEPTUAL: LO PRIVADO, LO INTIMO Y LO SECRETO

La exposición de motivos de la LOTARD elabora una teoría de la distinción entre la «intimidad» y la «privacidad». Ciertamente, la doctrina ha debatido la cuestión y por ello no puede sorprendernos. Lo que sí causa cierto estupor es que tras las disquisiciones doctrinales sobre el particular la LORTAD prescinda por completo de tales conceptos.

La utilización de los términos «privado» e «íntimo» ha dado lugar a grandes confusiones y discusiones. Lo *privado* se define en principio como oposición a lo común (6). Desde esta perpectiva, lo privado estaría conectado con el secreto en cuanto consecuencia de una acción de separar un determinado ámbito o conocimiento. No sólo con lo secreto, sino también con lo sagrado (*sacrum* y *secretum* arrancarían de *secernum* o separado) como advierte Durkheim (7). Lo privado sería así una noción de importante extensión. Y, en efecto, como sostiene Freund, lo privado no sería sinónimo de individual. Para Freund, puede contemplarse lo privado desde dos puntos de vista, desde el lado de lo público y desde el del individuo. Si bien desde el primer punto de vista lo privado aparece como la esfera de la interio-

(3) PABLO LUCAS MURILLO DE LA CUEVA: «La protección de los datos personales ante el uso de la informática», en *Anuario de Derecho Público y Estudios Políticos*, núm. 2 (1989-1990), págs. 153 y sigs.; íd.: «La protección de los datos personales ante el uso de la informática», en *RFDUC*, monográfico núm. 15 (1989), págs. 601 y sigs.

(4) Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

(5) STC 254/1993, de 20 de julio, Sala I (García-Mon), caso Olaverri.

(6) JULIEN FREUND: *L'essence du politique*, París, Sirey, 1981 (primera edición, 1965), pág. 282.

(7) Cit. por JAVIER DE LUCAS MARTÍN: «Democracia y transparencia. Sobre poder, secreto y publicidad», en *AFD* (1990), págs. 131 y sigs., pág. 137.

ridad y de la autonomía individuales, visto desde el lado del individuo designa aquello que en el individuo está vuelto hacia el exterior, hacia los otros. Este pensador considera que lo público y el Estado y el individuo como tal rara vez se enfrentan de forma directa, pues entre ambos existe la esfera de lo privado, formada *a la vez* de las relaciones íntimas del individuo con los otros y de las relaciones interindividuales y más impersonales de entre las asociaciones de diferente naturaleza de la sociedad civil donde se produce la dialéctica de lo privado y de lo público (8).

De parecido modo, Westin considera que la intimidad (*privacy*) puede manifestarse en cuatro situaciones básicas: soledad, «intimidad» (*intimacy*), anonimato y reserva. Por lo que aquí interesa, la segunda de esas situaciones, *intimacy*, se define porque el individuo actúa como parte de una pequeña unidad que reclama y está preparada para ejercer una segregación corporativa que permite alcanzar una relación franca, relajada y cerrada entre dos o más individuos (9). Se trataría también de una relación de tinte social, si bien se da la paradoja de que emplea unos vocablos, *intimacy* y *privacy*, de equívoca traducción.

A diferencia de lo privado que se definiría principalmente por un ámbito separado en el plano horizontal, lo *íntimo* se encuadraría más dentro de un plano vertical. El propio término íntimo da pie a ello. «Intimo» proviene del latín *intimus*, que es el superlativo de *interior* (10). Se trataría aquí del individuo en cuanto vuelto hacia su fuero interno o hacia aquello que hay en él de más singular, secreto, misterioso e incomunicable (11). Intimidad sería así un concepto superlativo más intenso que «privacidad», pudiendo ser considerado como una noción psicológica (12).

De acuerdo con lo anterior, pudiérase distinguir entre intimidad en sentido estricto y «privacidad» o lo privado en sentido más amplio como ámbitos diferentes pero consecuentes: lo íntimo sería un concepto estricto de dimensiones propiamente individuales y lo privado sería un ámbito que, abarcando lo íntimo, lo supera. En esta línea, algunos autores han reivindicado la distinción entre lo íntimo y lo privado, no sólo en el plano antropológico (13), sino también en el jurídico (14). Jurídicamente la distin-

(8) FREUND: *op. cit.*, pág. 309.

(9) ALAN F. WESTIN: *Privacy and Freedom*, Nueva York, Atheneum, sexta edición, 1970 (primera edición, 1967), pág. 31.

(10) FÉLIX GAFFIOT: *Dictionnaire Latin-Français*, París, Hachette, 1985 (primera edición, 1934), voz *intimus, -a, -um*.

(11) FREUND: *op. cit.*, pág. 309.

(12) HELENA BÉJAR MERINO: «La génesis de la *privacidad* en el pensamiento liberal», en *Sistema*, núm. 76 (1987), págs. 59 y sigs., pág. 65.

(13) NORBERTO GONZÁLEZ GAITANO: *El deber de respeto a la intimidad*, Pamplona, Eunsa, 1990, págs. 38 y sigs.

(14) CARLOS SORIA: «La información de lo público, lo privado y lo íntimo», en *Cuenta y Razón*, núms. 44-45 (1989), págs. 25 y sigs., pág. 25-26; GONZÁLEZ GAITANO: *op. cit.*, págs. 101 y sigs. No obstante, reconoce que salvo la LODHI ninguna otra norma española (ni constitucional ni legal) realiza esa distinción, al menos de forma expresa (*op. cit.*, págs. 111 y 113). Pudiera añadirse que una norma publicada con posterioridad, la LORTAD, sí distingue expresamente entre «privacidad» e «intimidad», pero sólo lo hace en la exposición de motivos. Recientemente, se adhiere a esa posición PABLO LUCAS MURILLO DE LA CUEVA: *Informática...*, págs. 29 y sigs.

ción sería relevante pues, según Hixon, la extensión interpretativa del contenido del derecho a la intimidad puede llevar a considerarlo como una *catch all phrase, protecting too little because it protects too much*, es decir, abarca mucho, pero aprieta poco (15).

Ahora bien, siguiendo a un sector autorizado de la doctrina (16), podría hablarse de intimidad en sentido amplio como lo comprensivo también de lo privado. Esta postura ha sido también acogida por el TC, para quien «el derecho constitucional a la intimidad excluye las intromisiones de los demás en la esfera de la vida privada personal y familiar de los ciudadanos» (17). Consideramos razonable esta posición. Por una parte, creemos que el entendimiento del derecho a la intimidad en un sentido amplio ofrece una categoría lo suficientemente flexible como para brindar una protección del más alto rango frente a ataques que puedan surgir por nuevos avances de la técnica que, en principio, son imprevistos para el legislador. Un buen ejemplo de ello lo ofrece el caso de la Genética en nuestros días, que es la nueva frontera del derecho a la intimidad, una vez que el Derecho ya ha colonizado el campo de la informática. Por otra, si consideramos determinados derechos como la inviolabilidad de domicilio, que tienen una faceta *ad extra* importante y los incluimos en el derecho a la intimidad, deberíamos defender entonces un concepto de intimidad en sentido amplio (18).

Creemos adecuado utilizar la noción de intimidad en ambos sentidos, pues no hay una regla fija al respecto y el sentido del concepto dependerá de las circunstancias. Así, por ejemplo, unas veces será procedente especificar que se usa el concepto estricto de intimidad. En este sentido, se puede apreciar que el derecho a la intimidad *stricto sensu* no puede ser objeto de suspensión, pero otros derechos que pertenecen al ámbito de lo privado (o a la intimidad *lato sensu*), como la inviolabilidad del domicilio y el secreto de las comunicaciones, sí lo son. Sin embargo, otras veces será útil emplear el concepto amplio de intimidad, como al considerar las nociones de intimidad informática o intimidad genética, o al hablar del secreto profesional. En estos supuestos, la utilización de este sentido lato permite abrir la posibilidad de muy importantes medios de garantía: reserva de ley, desarrollo por ley orgánica, respeto del contenido esencial del derecho, recurso de amparo, ordinario y constitucional, etc.

Debe hacerse una distinción final. Como ha puesto de manifiesto Goldschmidt, no se debe confundir la intimidad (o la vida privada) como algo atribuible a las personas con el secreto, cuyos beneficiarios son los poderes públicos, el Estado o una parte del mismo (sus aparatos represivos). En efecto, la extensión inconsiderada de los ámbitos políticos o estatales protegidos por el secreto perjudica, por un lado, a la publicidad entendida como control democrático, pero también, de otro lado, puede resultar lesiva para la intimidad al restringir aún más el ámbito de ésta (por ejemplo,

(15) RICHARD F. HIXON: *Privacy in a public society*, Nueva York-Londres, Oxford University Press, 1987, pág. 60 (cit. por LUCAS MURILLO: *Informática...*, pág. 29).

(16) WESTIN: *op. cit.*, págs. 31-32.

(17) ATC 221/1990 (FJ 3.º).

(18) Lucas Murillo considera, sin embargo, la inviolabilidad del domicilio como contenido del derecho a la intimidad *stricto sensu* (LUCAS MURILLO: *Informática...*, cit., pág. 29).

a través de las escuchas telefónicas «legales», pero no controladas por los jueces ni por la opinión pública, o a través del manejo de ciertos datos personales por los servicios secretos o la policía) (19). En el campo de la protección de datos personales la LORTAD ofrece demasiados ejemplos de la virtualidad deletérea de la intimidad privada que ejercen los secretos *públicos*, valga la expresión.

II. EL BIEN JURIDICO PROTEGIDO

A.1. Se ha planteado cuál es el bien jurídico protegido a través de las normas sobre el tratamiento automatizado de datos personales. La famosa sentencia del Tribunal Constitucional Federal Alemán de 15 de diciembre de 1983 configuró el llamado «derecho a la autodeterminación informativa» (*informationelle Selbstbestimmungsrecht*) en orden al tratamiento automatizado de datos personales. Para dicho Tribunal, del art. 2 GG dimana «la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida» (20).

Como tal categoría, se ha intentado por Lucas Murillo trasladarla a España con base en el art. 18.4 CE. Este autor considera que el derecho a la intimidad normalmente implica el poder jurídico de rechazar intromisiones ilegítimas en la esfera protegida y, correlativamente, determinar libremente y dentro de ella la propia conducta. Es un típico derecho de defensa. A su juicio, sin embargo, la técnica de la protección de datos es más complicada. De un lado, combina poderes del individuo frente a terceros (limitaciones, prohibiciones) con diversas garantías instrumentales. De otro lado, los datos que se protegen no tienen por qué ser íntimos, basta con que sean personales, aun cuando parezcan inocuos. De aquí que el ámbito de esta protección sea más amplio que el propio derecho a la intimidad (21).

Sobre estas premisas, Lucas Murillo afirma que en orden a proteger los datos personales frente a la informática conviene abandonar la referencia de la intimidad y enunciar un nuevo derecho —el derecho a la autodeterminación informativa—, que tendría como objeto preservar la información individual (íntima y no íntima) frente a su utilización incontrolada arrancando, precisamente, donde término el entendimiento convencional del derecho a la vida privada (22). Estas diferencias explicarían que ciertos autores adjetiven la intimidad, distinguiendo la intimidad «física» o clásica (libertad frente a toda intromisión sobre uno mismo, su casa, familia, comunicaciones o relaciones) de la intimidad «informativa» (derecho a determinar cómo

(19) MAURE L. GOLDSCHMIDT: «Publicity, privacy and secrecy», en *WPQ*, vol. VII, núm. 3 (1954), págs. 401 y sigs., pág. 411.

(20) STCFA de 15 de diciembre de 1983, *BVerfGE*, t. 65, págs. 1 y sigs. Hay traducción castellana de Mariano Daranas, en *Boletín de Jurisprudencia Constitucional*, núm. 33 (1984), págs. 126 y sigs.

(21) LUCAS MURILLO: *El derecho...*, págs. 117-118; íd.: *Informática...*, págs. 27 y sigs.

(22) LUCAS MURILLO: *El derecho...*, pág. 120; íd.: *Informática...*, págs. 32-33.

y en qué medida se puede comunicar a otros información sobre uno mismo) (23). La propuesta de Lucas Murillo ha encontrado eco en buen número de autores, aunque, como veremos, la jurisprudencia española no la ha acogido.

A.2. Siendo lo apuntado cierto, creemos que una serie de elementos de juicio puede conducir a una tesis más matizada. En primer lugar, ya Warren y Brandeis definieron la intimidad como «el derecho del individuo de determinar, *ordinariamente*, en qué medida sus pensamientos, sentimientos y emociones deben ser *comunicados* a otros» (24), o lo que es lo mismo, «decidir si lo que es suyo puede darse al público» (25). Westin va un poco más allá formulando una definición de intimidad como la pretensión (de un individuo, grupo o institución) de determinar por sí mismo cuándo, cómo y en qué grado puede comunicarse a otros *información* sobre él (26). Otros autores americanos realizan afirmaciones coincidentes (27). En Europa, Schmitt Glaeser ha afirmado que la protección de la esfera de la vida privada puede calificarse como «protección de la información» (28). Algunos autores españoles también proponen definiciones similares (29). Esta definición de intimidad formulada por estos autores es muy coincidente con la definición de autodeterminación informativa consagrada por el TCFA en su famosa sentencia sobre la ley del censo.

En segundo lugar, es preciso advertir que *junto a* la concepción clásica del derecho a la intimidad a partir de la teoría de las esferas, en la que lo íntimo correspondería al círculo concéntrico más interno y lo privado a un círculo más amplio, se ha formulado una nueva concepción a partir de la teoría del mosaico. Considerando la insuficiencia de la teoría de las esferas para hacer frente a ciertas nuevas formas

(23) LUCAS MURILLO: *El derecho...*, pág. 121.

(24) SAMUEL D. WARREN y LOUIS D. BRANDEIS: «The right to privacy», en *HLR*, vol. IV, núm. 5 (15 de diciembre de 1890), págs. 193 y sigs., pág. 198.

(25) WARREN y BRANDEIS: *op. cit.*, pág. 199.

(26) WESTIN: *op. cit.*, pág. 7.

(27) Así, Fried la define como «control sobre la información que nos concierne» y Parker como «control sobre cuándo y quién puede percibir diferentes aspectos de nuestra persona», cit. por LUIS GARCÍA SAN MIGUEL RODRÍGUEZ-ARANGO: «Reflexiones sobre la intimidad como límite de la libertad de expresión», en L. GARCÍA SAN MIGUEL (ed.): *Estudios sobre el derecho a la intimidad*, Madrid, Tecnos, 1992, págs. 15 y sigs., pág. 17.

(28) WALTER SCHMITT GLAESER: «Schutz der Privatsphäre», en JOSEF ISENSEE y PAUL KIRCHHOF (eds.): *Handbuch des Staatsrechts der Bundesrepublik Deutschland*, tomo II, Heidelberg, C. F. Müller, 1989, págs. 41 y sigs., pág. 44.

(29) Nogueroles distingue un concepto estático (exclusión del conocimiento ajeno) y uno dinámico (control de las informaciones referentes a uno mismo) de intimidad. Ambas, sobre todo la segunda, se pueden reconducir a la noción de autodeterminación informativa (vid. NICOLÁS NOGUEROLES PEIRÓ: «La intimidad económica en la doctrina del Tribunal Constitucional», en *REDA*, núm. 52 [1986], págs. 559 y sigs., págs. 560-561). Salvador Coderch, aunque parte de la noción de intimidad de Prosser, se pregunta qué tienen de común los cuatro contenidos que ese autor norteamericano atribuye a la intimidad, para contestarse que «tal vez, sólo la idea de que las personas deben tener un derecho a controlar ciertas informaciones sobre ellas mismas», si bien el problema «es saber cuáles sean éstas» (PABLO SALVADOR CODERCH: *El mercado de las ideas*, Madrid, CEC, 1990, pág. 319).

sofisticadas de ataque que pueden afectarla, Madrid Conesa ha postulado la que llama teoría del mosaico. Esta teoría estima lo privado y lo público como conceptos relativos. De ahí concluye, en primer lugar, que lo privado y lo público son relativos en función de quién sea el otro sujeto en la relación informativa, y en segundo lugar, que existen datos *a priori* irrelevantes desde el punto de vista del derecho a la intimidad y que, sin embargo, en conexión con otros, quizá también irrelevantes, pueden servir para hacer totalmente transparente la personalidad de un ciudadano «al igual que ocurre con las pequeñas piedras que forman los mosaicos, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado» (30).

No podemos compartir, sin embargo, la idea de que lo privado sea relativo. Lo es sólo relativamente, valga la redundancia. Sigue habiendo aspectos que objetivamente, sustancialmente, son íntimos o privados y, en consecuencia, son merecedores de tutela. Quizá lo que es relativo es lo público, con la consecuencia de que hay ciertos datos públicos que pueden tener una trascendencia para la intimidad si se conectan entre sí. Se produciría una suerte de metamorfosis que convierte los datos públicos en privados o íntimos. Lo cierto es que la teoría del mosaico permite dar cabida a los problemas que suscita la intimidad informática.

En tercer lugar, la consideración de que es el derecho a la intimidad (vida privada) el que se halla principalmente afectado por las técnicas de proceso de datos se halla expuesta en el Convenio del Consejo de Europa sobre este asunto (31), así como por diversos autores (32).

Finalmente, en cuarto lugar, creemos con Schmitt Glaeser que un derecho como la intimidad debe permanecer abierto, flexible y capaz de acomodación para ulteriores desarrollos en orden a otorgar protección frente a las nuevas situaciones de peligro que puedan surgir con el desarrollo técnico y social (33). En este sentido, el TCFA ha indicado que el art. 2.1 GG, en relación con el art. 1.1 GG, permite fundar un derecho a la protección de la vida privada con sustantividad propia que opera como una cláusula general y subsidiaria que entra en juego a falta de concreciones del mismo mediante derechos especiales expresamente regulados (34). Por lo demás, el propio Lucas Murillo reconoce la filiación del derecho a la autodeterminación informativa del derecho a la intimidad (35).

Desde esta perspectiva, el derecho a la autodeterminación informativa no sería tanto un nuevo derecho que comienza allí donde termina el derecho a la intimidad

(30) FULGENCIO MADRID CONESA: *Derecho a la intimidad, informática y Estado de Derecho*, Valencia, Universidad de Valencia, 1984, pág. 45.

(31) Preámbulo y art. 1 del Convenio 108 del Consejo de Europa.

(32) GIUSEPPE MIRABELLI: «Problemi legislativi dell'attuazione del diritto alla privacy», en GUIDO GERIN (dir.): *Les effets de l'informatique sur le droit à la vie privée*, Padua, CEDAM, 1990, págs. 43 y sigs.; JACQUES FAUVET: «La protection du droit à la vie privée», en GERIN: *op. cit.*, págs. 55 y sigs., pág. 57 (Fauvet es presidente de la Comisión nacional francesa de la informática y la libertad).

(33) SCHMITT GLAESER: «Schutz...», pág. 58.

(34) Sentencia del TCFA, de 16 de enero de 1957, *BVerfGE*, t. 6, págs. 32 y sigs., pág. 36.

(35) LUCAS MURILLO: *Informática...*, pág. 29.

cuanto el mismo derecho a la intimidad auxiliado de nuevas técnicas y aplicado a un nuevo objeto, la informática (36).

B.1. El recurso al art. 10.2 CE nos lleva a considerar la jurisprudencia del TEDH (*). Este, al menos parcialmente, vincula el derecho a la protección de la vida privada (art. 8 CEDH) con determinados aspectos del derecho a la autodeterminación informativa o a la protección frente al manejo de datos personales por la informática (37).

Acerca del principio de lealtad en la obtención de los datos (38), el juez francés del TEDH Pettiti ha señalado las conexiones de la protección frente a las escuchas telefónicas *ex* art. 8 CEDH y el derecho a la intimidad informática y a la protección de datos personales. En su opinión, no se puede separar el tema de las escuchas del de los bancos de datos, puesto que las escuchas tienen como consecuencia el registro y archivo de las informaciones obtenidas. Es decir, que podríamos decir que aquí se encuentran problemas relacionados con el principio de lealtad en la obtención de datos. Pettiti cita expresamente el Convenio de 1981 y sostiene que las escuchas telefónicas reclaman una serie de contramedidas, entre las que menciona el derecho de personarse en el que se incluye la facultad de impugnar los datos obtenidos y el de conocer la existencia de los datos y de los bancos en que están registrados (39).

En segundo lugar, por lo que hace al principio de publicidad, el almacenamiento de datos relativos a la vida privada en un registro secreto de la policía, así como su cesión y la negativa de permitir al afectado refutar esos datos supone una injerencia en el derecho al respeto de la vida privada, reconocido en el art. 8.1 CEDH (40). Ello no obstante, el TEDH, en una interpretación estricta del Convenio de Roma, considera que tal injerencia es conforme al art. 8.2 CEDH por cuanto los intereses de la seguridad nacional prevalecen sobre los intereses individuales del afectado (41). No obstante, para los jueces Pettiti y Russo se manifiesta la necesidad de que el individuo pueda disponer de un recurso contra una inscripción que sea el resultado de un error fundamental, incluso si se mantiene el secreto

---

(36) Esta parece ser la postura de ANTONIO TORRES DEL MORAL: *Principios de Derecho constitucional español*, tomo I, Madrid, Facultad de Derecho, UCM, tercera edición, 1992, pág. 401; ENRIQUE ALVAREZ CONDE: *Curso de Derecho constitucional*, vol. I, Madrid, Tecnos, 1992, págs. 295-296; FRANCISCO FERNÁNDEZ SEGADO: *El sistema constitucional español*, Madrid, Dykinson, 1992, pág. 221; JORGE DE ESTEBAN y PEDRO J. GONZÁLEZ-TREVIJANO: *Derecho constitucional español*, tomo II, Madrid, Facultad de Derecho, UCM, 1993, págs. 107-108.

(*) He tratado esta cuestión en *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, Civitas, Madrid, 1994, págs. 49 y sigs.

(37) SSTEDH Leander, A 116, núm. 48; Gaskin, A 160, núm. 39. Por ello, debería matizarse el juicio de Rodríguez-Piñero, para quien «el *habeas data* no estaba ni siquiera implícito en el Convenio de Roma» (VP a la STC 254/1993). El TEDH, al menos, lo considera incluido, siquiera fragmentariamente en el art. 8 CEDH.

(38) Reconocido en el art. 5.a del Convenio 108.

(39) Opinión concordante del juez Pettiti a la STEDH Malone, A 82.

(40) STEDH Leander, A 116, núm. 48.

(41) STEDH Leander, A 116, núm. 47.

sobre el origen de la información (42). Están aquí implicados el principio de publicidad por una parte y el principio de acceso a los datos y de corrección de errores por otra (43). Debe advertirse que el TEDH rechaza que el derecho a recibir informaciones garantizado por el art. 10 sea aplicable al acceso a registros públicos de informaciones, pues el TEDH lo configura no tanto como un derecho de prestación cuanto como un derecho a que el Estado se abstenga de impedir que una persona reciba información que otros aspiran o consienten en facilitar (44).

Finalmente y por lo que hace al principio de acceso individual a los datos (45), el TEDH afirma que, sin duda, los documentos incluidos en el fichero del caso litigioso conciernen a la «vida privada y familiar» del reclamante en un grado tal que el problema de su accesibilidad al interesado entra en el terreno del art. 8 CEDH. Ahora bien, el Tribunal se previene frente a posibles acusaciones de «activismo» judicial en este terreno afirmando que lo anterior no decide la cuestión de saber si los derechos generales pueden deducirse del art. 8.1 CEDH, pues alega que no está llamado a decidir en abstracto los grandes problemas de principio en estas materias, sino a decidir sobre el caso concreto del demandante (46). En el caso de autos, las informaciones recogidas y conservadas por la autoridad afectaban a la identidad fundamental del demandante y proporcionaban el único recuerdo coherente de su infancia y de sus años de formación, por lo que el rechazo a dejarle consultar el fichero entrañaba una lesión de su derecho al respeto de su vida privada (47). En definitiva, pese a las reservas que formula el TEDH aquí, lo cierto es que el art. 8 CEDH protege, al menos fragmentariamente, el derecho a la intimidad informática.

B.2.a. La jurisprudencia del Tribunal Constitucional parece inclinarse por una línea de autorrestricción (*self restraint*) al reconocer derechos fundamentales. De acuerdo con la misma, parece que sólo los derechos concretamente plasmados en la Constitución pueden gozar de la cobertura propia de los derechos fundamentales. A juicio del Alto Tribunal, ciertamente «es indudable que muchos de los derechos fundamentales y libertades públicas tutelables en amparo son proyecciones del valor libertad, pero sólo estas proyecciones concretas crean derechos amparables en esta vía procesal (el amparo constitucional)». En particular, niega el TC que la dignidad, reconocida expresamente en el art. 10.1 CE, pueda ser en sí misma un derecho fundamental al margen de los derechos fundamentales expresamente previstos en la Constitución. Para el Tribunal, «sólo en la medida en que tales derechos sean tutelables en amparo y únicamente con el fin de comprobar si se han respetado las exigencias que no en abstracto, sino en el concreto ámbito de cada uno de aquéllos, deriven de la dignidad de la persona habrá de ser ésta tomada en consideración por este Tribunal como referente». En cambio, la dignidad no puede ser tomada en con-

(42) Opinión concordante de los jueces Pettiti y Russo a la STEDH Leander, A 116.
(43) Reconocidos en el art. 8.a-b-c del Convenio 108.
(44) SSTEDH Leander, A 116, núm. 74; Gaskin, A 160, núm. 51.
(45) Art. 8.b del Convenio 108.
(46) STEDH Gaskin, A 160, núm. 37.
(47) STEDH Gaskin, A 160, núm. 39.

sideración «de modo autónomo para estimar o desestimar las pretensiones de amparo que ante él (el TC) se deduzcan» (48).

A la vista de esta jurisprudencia creemos que la pretensión de construir un derecho fundamental *distinto* de los expresamente recogidos por la Constitución resulta sumamente problemática. En efecto, es probable que, si no hay conexión directa con alguno de los derechos fundamentales consagrados por la CE, ese derecho *nuevo* que queramos elaborar pueda verse privado de la significación propia de los derechos fundamentales, con todo lo que ello implica (ausencia de amparo constitucional, etc.). Se podría alegar, ciertamente, que el art. 18.4 CE reconoce un derecho. Sin embargo, parece que puede convenirse en que ese precepto establece un límite a un derecho (el uso de la informática) para garantizar otros derechos (entre los que se menciona expresamente el honor y la intimidad personal y familiar), de forma bastante similar a lo que sucede, por ejemplo, con el art. 20.4 CE. Desde esta perspectiva, si queremos dotar a la protección de los datos personales de las más elevadas garantías, quizá más útil y más seguro que considerarla incluida en un derecho nuevo, pueda ser el estimarla comprendida en un derecho fundamental ya reconocido. Ese derecho parece que debiera ser la intimidad.

b. El TC se ha pronunciado escasas veces sobre la relación entre la informática y la intimidad. En la primera ocasión, manifestó que en nada atenta, en principio, a la intimidad personal el que los datos que deben suministrarse a la Hacienda Pública se ofrezcan a través de medios informatizados, ya que sólo su uso más allá de lo legalmente autorizado (49) podría constituir un grave atentado a los derechos fundamentales de las personas, lo que, caso de producirse, podría ser objeto de la correspondiente demanda de amparo (50). El pronunciamiento es escueto, pero no por ello exento de crítica. En efecto, parece excesivamente restrictivo hablar del uso «legalmente autorizado» como criterio de medida de las violaciones del artículo 18.4 CE, pues en tanto esa ley no se dicte la protección no existiría. Sería más correcto hablar de uso «constitucionalmente autorizado», lo que permitiría el adecuado amparo de este derecho. Por otra parte, pese a la parquedad de las palabras, parece que el TC no identifica el art. 18.4 con el art. 18.1, aunque tampoco lo considera un derecho fundamental autónomo, nuevo.

La cuestión se ha tratado con mayor profundidad en la reciente decisión del caso Olaverri. La postura del TC es ligeramente vacilante. Por una parte, se dice que el art. 18.4 CE es un instituto de garantía de otros derechos, especialmente el honor y la intimidad, pero también «un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento

(48) STC 120/1990, de 27 de junio, Pleno (García-Mon, Díaz, Gimeno), FJ 4.º En una línea restrictiva próxima, la STC 184/1990, de 15 de noviembre, Pleno (Leguina), FJ 2.º

(49) Se aludiría aquí al principio de calidad de los datos, previsto en el art. 5 del Convenio 108 del Consejo de Europa.

(50) ATC 642/1986 (FJ 3.º).

mecanizado de datos» (51). Esto supondría identificar el art. 18.4 con un derecho nuevo que, por lo demás, no se califica como «derecho a la autodeterminación informativa» (las partes en el proceso tampoco lo calificaron así).

Ahora bien, la misma sentencia, frente a lo anterior, contiene numerosos asertos en los que se afirma que lo protegido en el art. 18.4 CE es el derecho a la intimidad. La sentencia recuerda que el propio Convenio 108 del Consejo de Europa garantiza el respeto de los derechos y libertades fundamentales, y en especial el derecho a la vida privada, respecto al tratamiento automatizado de sus datos personales (52). De forma más directa, el TC declara que «la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona». A su juicio, «la protección de la intimidad de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las Administraciones Públicas conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales en poder de las autoridades». Para el TC, la constatación de que los datos personales que almacena la Administración son utilizados por sus autoridades y sus servicios, «impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión». Según el TC, las facultades de información precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de la Administración donde obran datos de un ciudadano «son absolutamente necesarios para que los intereses protegidos por el art. 18 CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos», pues «forman parte del contenido del derecho a la intimidad» (53).

En definitiva, creemos que el TC considera el art. 18.4 como una indicación expresa del contenido esencial del derecho a la intimidad, por lo que, a nuestro juicio, es conveniente la expresión «intimidad informática» para aludir a ese contenido particular del derecho a la intimidad. Esta conexión facilita muchos problemas que plantea el ejercicio de la protección de datos frente al uso de la informática; así, entre otros: en primer lugar, el rango de la ley (orgánica) que desarrolle este derecho; en segundo lugar, la posibilidad de acudir al amparo ordinario, o en tercer lugar, la posibilidad del recurso de amparo constitucional (buen ejemplo de ello es la STC 254/1993, dictada para resolver un caso de protección de datos sin la cobertura de la LORTAD).

III. LA NATURALEZA JURIDICA DEL DERECHO

A. Peter Häberle ha examinado los derechos fundamentales desde una doble perspectiva: de un lado, como garantías de la libertad individual (derechos de defensa); de otro, como instituciones que hacen operativos los contenidos de los derechos

(51) STC 254/1993 (FJ 6.º).

(52) STC 254/1993 (FJ 4.º). Art. 1 del Convenio 108 del Consejo de Europa.

(53) STC 254/1993 (FJ 7.º, y en el mismo sentido, los FFJJ 8.º y 9.º).

para la consecución de los fines sociales y colectivos constitucionalmente proclamados. Pérez Luño, siguiendo a este autor, afirma que la dimensión institucional u objetiva de los derechos fundamentales obliga a considerar a éstos también como derechos de participación, reconociendo a los ciudadanos un *status activus processualis* que les permite la tutela jurisdiccional efectiva de todos los derechos fundamentales (54).

Baño León entiende esta naturaleza institucional del derecho fundamental como la garantía positiva de ámbitos de actuación del particular, aseguramiento de la pervivencia de determinadas organizaciones (55) o el reconocimiento de ciertos procedimientos para realizar en la práctica los derechos (56). Se trata de instituciones orientadas a tutelar la libertad (57).

La legislación ha conformado el derecho a la intimidad informática desde estas ambas perspectivas. En efecto, el derecho a la intimidad informática comprende una serie de deberes positivos por parte de los poderes públicos e instituciones privadas que procedan al tratamiento automatizado de datos personales. Es lo que se entiende por la calidad de los datos, la cual comprende la obligación de que los datos no puedan utilizarse para finalidades distintas de aquellas para que los datos se hubieran recogido; la necesidad de veracidad, exactitud y puesta al día de los datos; el deber de almacenamiento de los datos de forma que permita el ejercicio del derecho de acceso por medio del afectado, y el derecho al olvido o a que no puedan ser registrados ciertos datos adversos (58).

La normativa instituye varios organismos encargados de velar por el correcto uso de los medios informáticos en el procesamiento de datos personales. Entre estos organismos puede citarse al Comité Consultivo europeo (59), de magras competencias, a la Agencia de Protección de Datos Personales (60) o a la «autoridad de control común» prevista en el Acuerdo de Schengen (61). También se crean diversos procedimientos para asegurar la tutela del derecho (62).

En este terreno conviene tener muy en cuenta que el derecho a la intimidad, del que deriva la protección que ofrece la LORTAD, tiene una importantísima dimen-

---

(54) Cit. por ANTONIO ENRIQUE PÉREZ LUÑO: *Derechos humanos, Estado de Derecho y Constitución*, Madrid, Tecnos, 1984, pág. 300.

(55) JOSÉ MARÍA BAÑO LEÓN: «La distinción entre derecho fundamental y garantía institucional en la Constitución española», en *REDC*, núm. 24 (1988), págs. 155 y sigs., pág. 170.

(56) BAÑO LEÓN: *op. cit.*, pág. 160. Aparicio preconiza esto en relación al derecho a la tutela judicial (vid. MIGUEL ANGEL APARICIO PÉREZ: «El derecho a la organización de la tutela judicial efectiva», en *ADCP*, núm. 1 (1988), págs. 77 y sigs.

(57) LUIS AGUIAR DE LUQUE: «Dogmática y teoría jurídica de los derechos fundamentales en la interpretación de éstos por el Tribunal Constitucional español», en *RDP*, núms. 18-19 (1983), págs. 17 y sigs., pág. 22.

(58) Art. 5 del Convenio 108 del Consejo de Europa; arts. 4 y 28.3 LORTAD; arts. 102 y sigs. del Convenio de Schengen.

(59) Art. 18 y sigs. Convenio 108 del Consejo de Europa.

(60) Arts. 34 y sigs. LORTAD.

(61) Art. 115 del Convenio de Schengen.

(62) Art. 16 LORTAD.

sión democrática. Ha sido Schmitt Glaeser quien ha subrayado esta *dimensión institucional democrática* del derecho a la intimidad, además de su faceta de derecho de defensa. La dimensión defensiva del derecho a la intimidad no debe llevar a una errónea concepción conforme a la cual la esfera privada no genera ningún fruto para la comunidad estatal. La protección de la intimidad «hace posible el desarrollo, el fortalecimiento y la recuperación de la identidad personal y, como consecuencia de ella, de una actividad social que, partiendo de la especificidad del individuo, conduce a aquella configuración diversa y original de la comunidad que sustancialmente caracteriza a una democracia viva» (63).

Desde esta perspectiva, el derecho a la intimidad no es sólo un derecho fundamental de defensa, sino también una garantía institucional, o mejor, objetiva del pluralismo y de la democracia. Un sistema que no garantice adecuadamente el derecho a la intimidad pudre las raíces que lo nutren. Para que una democracia esté viva, es preciso que respete la intimidad de quienes la componen, pues sólo así, desde la libertad e independencia de cada ciudadano, puede construirse una sociedad libre. Esta dimensión democrática no ha sido acogida aún por el TC al tratar del derecho a la intimidad (64).

B. El TEDH ha configurado el derecho al respeto de la vida privada como un derecho positivo, de prestación, además de como un derecho de defensa. Ahora bien, estima que existe un amplio margen de apreciación del Estado para decidir, de acuerdo con las necesidades y los medios de la sociedad y de las personas, las medidas que se deben adoptar para asegurar el cumplimiento del Convenio entendido como cumplimiento de una obligación positiva (65). De igual modo, ese Tribunal ha llevado a cabo una configuración institucional de tal derecho al estimar que el respeto al mismo puede exigir la presencia de determinados procedimientos y garantías (66).

Este planteamiento ha sido acogido por la jurisprudencia constitucional. El TC ha manifestado expresamente que el art. 18.1 y 4 CE no incluye solamente un derecho de defensa frente al Estado, sino que también supone deberes positivos por parte del Estado (67). En efecto, puede decirse por analogía de lo que el TC dice respecto al derecho a la vida, que los derechos fundamentales, por una parte, en cuanto derechos subjetivos, dan a sus titulares la posibilidad de recabar el amparo judicial frente a toda actuación de los poderes públicos que amenace el bien protegido en el

(63) SCHMITT GLAESER: «Schutz...», pág. 43.

(64) En particular ignora el TC esta dimensión institucional democrática en los casos de conflicto con las libertades de expresión e información a las que sí atribuye dicha dimensión.

(65) SSTEDH Marckx, A 31, núm. 31; Airey, A 32, núm. 32; X e Y, A 91, núm. 23; Abdulaziz, A 94, núm. 35; Rees, A 106, núm. 37; Eriksson, A 156, núm. 71; Gaskin, A 160, núm. 38 y 42; Powell y Rayner, A 172, núm. 41; Cossey, A 184, núm. 37; B. contra Francia, A 232-C, núm. 44.

(66) SSTEDH W. contra el Reino Unido, A 121-A, núm. 36; B. contra el Reino Unido, A 121-B, núm. 65; R. contra el Reino Unido, A 121-C, núm. 69; Olsson, A 130, núm. 71; Kruslin, A 176-A, núm. 36; Huvig, A 176-B, núm. 36.

(67) STC 53/1985 (FJ 4.º).

derecho; pero, por otra parte, también imponen a los poderes públicos, y en especial al legislador, el deber de adoptar las medidas necesarias para proteger ese bien frente a los ataques de terceros sin contar para ello con la voluntad de sus titulares. Tienen, por tanto, un contenido de protección positiva (68).

El derecho a la intimidad informática también ha sido considerado por el TC desde una perspectiva positivo-institucional. Según el Tribunal, además del elemento negativo más «elemental» de este derecho, que significa el ser un límite para el uso de la informática, «la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria». Por ello, «la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona». Para el TC, «la protección de la intimidad de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las Administraciones públicas conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales en poder de las autoridades». De aquí que puedan establecerse ciertas exigencias: «toda la información que las Administraciones públicas recogen y archivan ha de ser necesaria para el ejercicio de las potestades que les atribuye la Ley y ha de ser adecuada para las legítimas finalidades previstas por ella». En conclusión, «las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración pública donde obran datos personales de un ciudadano son absolutamente necesarios para que los intereses protegidos por el art. 18 CE y que dan vida al derecho fundamental a la intimidad resulten real y efectivamente protegidos». Por ende, «dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente» (69).

IV. LOS SUJETOS

A. *Sujetos activos*

Como indica Lucas Murillo no hay problema alguno en atribuir este derecho a los extranjeros, pues la LORTAD atribuye el derecho a las «personas físicas», sin distinción de nacionalidad (70). Lucas Murillo y Pérez Luño admiten la posibilidad doctrinal de reconocer la titularidad por personas jurídicas del derecho a la intimidad informática (71). A juicio de Lucas Murillo, dado que las personas jurídicas no

(68) SSTC 53/1985 (FJ 4.º); 120/1990 (FJ 7.º); 137/1990 (FJ 5.º); 11/1991 (FJ 2.º). En contra, VP de Rubio a STC 53/1985. Todas sobre el derecho a la vida.

(69) STC 254/1993 (FJ 7.º).

(70) LUCAS MURILLO: *Informática...*, pág. 49.

(71) LUCAS MURILLO: *El derecho...*, págs. 181-182; ANTONIO ENRIQUE PÉREZ LUÑO: «Los derechos humanos en la sociedad tecnológica», en M. LOSANO y otros: *Libertad informática y leyes de protección de datos*, Madrid, CEC, 1990, pág. 154.

son sino instrumentos de los que se valen los hombres para alcanzar determinados fines que de otro modo serían de más difícil consecución, puede considerarse que hay importantes argumentos a favor de ese reconocimiento. Ahora bien, como recoge el indicado autor, la LORTAD ha rechazado expresamente la posibilidad de reconocer este derecho a la intimidad informática a las personas jurídicas, siguiendo el criterio defendido en algunos países (Alemania, Francia, Irlanda...) y rechazando la posición de otros que sí admiten tal reconocimiento (Austria, Dinamarca, Islandia...) (72). Por otro lado, en el marco especial del sistema de Schengen, la protección de los datos se articula a través de diversos derechos que se atribuyen a «toda persona» (73). Ahora bien, todos los datos que se someten al tratamiento del Sistema de Información de Schengen son datos referidos a personas individuales (74).

B. *Sujetos pasivos*

1) *Poderes públicos*

a) La normativa vigente centra su atención en los poderes públicos. La LORTAD rige, en principio, respecto a los ficheros automatizados de datos de carácter personal del sector público. En este sentido, en un primer nivel, todos los que *intervengan en cualquier fase* del tratamiento de los datos personales se encuentran sujetos a la normativa. Los pertenecientes a este grupo se hallan obligados al secreto profesional respecto de tales datos y al deber de guardarlos, obligaciones que subsisten aun después de finalizar sus relaciones con el titular del fichero automatizado o con el responsable del mismo (75).

En un segundo nivel, más riguroso, se halla sometido a la disciplina de la LORTAD todo responsable de un fichero de esas características, es decir, toda persona física o jurídico-pública u órgano administrativo que *decida* sobre la finalidad, contenido y uso del tratamiento de datos (76).

Por su parte, el Convenio de Schengen crea un sistema de información común denominado Sistema de Información de Schengen (SIS). A tal efecto, cada Estado debe crear y mantener por su cuenta y riesgo su parte nacional del SIS, cuyo fichero de datos deberá ser materialmente idéntico a los ficheros de datos de la parte nacional de cada una de las otras partes contratantes mediante el recurso a una unidad de apoyo técnico (77). En consecuencia, es claro que los ficheros del SIS son de titularidad pública.

Los responsables de ficheros de titularidad pública deben cumplir con una serie

(72) Art. 1 LORTAD; LUCAS MURILLO: *Informática...*, págs. 49 y sigs.
(73) Arts. 109-111 del Convenio de Schengen.
(74) Art. 94 del Convenio de Schengen.
(75) Art. 10 LORTAD.
(76) Art. 3.d LORTAD.
(77) Art. 92 del Convenio de Schengen.

de principios. En primer lugar, el de calidad de los datos, en virtud del cual sólo se pueden recoger y procesar datos personales cuando sean adecuados, pertinentes, no excesivos en relación con el ámbito y las finalidades legítimas para las que se han obtenido, utilizables sólo para la finalidad con la que se recogieron, exactos y actualizados, debiéndose cancelar los que hayan dejado de ser necesarios (78).

En segundo lugar, el principio de información en la recogida de datos, conforme al que debe informarse de forma expresa, precisa e inequívoca a aquellos a quienes se soliciten datos personales de la existencia del fichero y de la identidad y dirección del responsable del mismo, de la obligatoriedad o no de proporcionar los datos y de las consecuencias de su negativa a darlos y de los derechos que le asisten (79). Estos derechos son: el de impugnación de las valoraciones realizadas sólo sobre datos informáticos; el de información, pudiendo averiguar la existencia de ficheros de datos personales, sus finalidades y la identidad de los responsables; el de acceso, por el que se le habilita para solicitar y obtener información de sus datos personales incluidos en ficheros automatizados; el de rectificación y cancelación de los datos personales que resulten inexactos o incompletos (80).

En tercer lugar, el principio del consentimiento, por el que, en principio, el tratamiento informático de datos personales requiere el consentimiento del afectado. Sin embargo, existen algunos datos para los que no se precisa el consentimiento. Es el caso de los datos de carácter personal que se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias o cuando se refieran a personas vinculadas por una relación negocial, laboral, administrativa o contractual y sean necesarias para el mantenimiento de tales relaciones (81).

En cuarto lugar, el principio de seguridad de los datos en cuya virtud deben adoptarse las medidas necesarias para evitar la alteración, pérdida o tratamiento o acceso no autorizados (82).

En quinto lugar, el principio del deber de secreto profesional, similar al que recae sobre todos los que intervienen en el tratamiento de los datos.

b) La normativa vigente, sin embargo, deja a los poderes públicos amplios espacios inmunes a la acción protectora del derecho a la intimidad informática. La LORTAD y el Convenio de Schengen establecen unos límites al derecho a la intimidad informática o excepciones a estos principios; en concreto, al principio del consentimiento, que son numerosos, quizá excesivos.

b.I. La LORTAD establece diversas restricciones. En primer lugar, es posible que una serie de los llamados datos «sensibles» (origen racial, salud y vida sexual) puedan ser recabados, tratados y cedidos sin consentimiento del afectado «cuando

(78) Art. 4 LORTAD; Arts. 99.1 y 105-106 del Convenio de Schengen.
(79) Art. 5 LORTAD.
(80) Arts. 12-15 LORTAD.
(81) Arts. 6 y 11 LORTAD.
(82) Art. 9 LORTAD.

por razones de interés general general así lo disponga una ley» (83). Por un lado, es difícil determinar qué es el «interés general», pues, en principio, la política trata de lo común, de lo que es de interés general, por lo que toda ley parece que se dicta en interés general. Por otro lado, en este caso en el que están en juego datos «sensibles» creemos que dicha ley debiera tener el carácter de orgánico, pues supone un claro desarrollo restrictivo del derecho a la intimidad (84).

En segundo lugar, la LORTAD permite la cesión de datos personales de forma heterodoxa en dos supuestos. Por un lado, los datos personales obtenidos para una finalidad determinada pueden ser cedidos al responsable de otro archivo cuando una ley así lo prevea (85). Este precepto creemos que es inconstitucional porque permite un vaciamiento del derecho a la intimidad informática. Es incluso posible que datos «sensibles» obtenidos merced a una ley dictada «por razones de interés general» puedan ser cedidos, sin consentimiento del afectado, en virtud de una nueva ley (ordinaria) que ni siquiera debe justificarse en «razones de interés general». Por otro lado, es posible la cesión de datos personales entre Administraciones públicas si dicha cesión «hubiese sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso» (86). Según Lucas Murillo, esa disposición no puede tener naturaleza reglamentaria y debe ser de carácter legal (87).

En tercer lugar, la LORTAD excluye el derecho de información del afectado en la recogida de los datos cuando esa información «impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la Seguridad pública o a la persecución de infracciones penales o administrativas» (88). La alusión a las infracciones administrativas, no mencionada en el Convenio europeo (89), vulnera frontalmente el mismo en cuanto que permite que los Estados brinden una protección más amplia de la intimidad informática, pero no que rebajen el nivel ofrecido en el mismo (90). Esta extensión a las infracciones administrativas de la restricción del derecho ha sido objeto de sospechas de posible inconstitucionalidad (91).

En cuarto lugar, se excluyen los derechos de acceso, rectificación y cancelación si, «ponderados los intereses en presencia», resultase que tales derechos «hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección». En este supuesto, el órgano administrativo responsable del fichero dictará resolución motivada. El precepto ha sido severamente criticado. Por un lado,

(83) Art. 7.3 LORTAD.
(84) En el mismo sentido, LUCAS MURILLO: *Informática...*, pág. 71.
(85) Art. 11.2.a LORTAD.
(86) Arts. 11.2.e y 19.1 LORTAD.
(87) LUCAS MURILLO: *Informática...*, pág. 98.
(88) Art. 22.1 LORTAD.
(89) Art. 9.2.a del Convenio 108.
(90) Art. 11 del Convenio 108.
(91) LUCAS MURILLO: *Informática...*, pág. 101.

existe una grave indeterminación de cuáles son esas «razones de interés público» o esos «intereses de terceros». Por otro, la necesidad de motivación como única garantía parece muy insuficiente (92). Esta exclusión, por tanto, también proporciona dudas sobre su constitucionalidad.

En quinto lugar, también desaparecen los derechos de acceso, rectificación y cancelación ante la Hacienda Pública. Los responsables de sus ficheros pueden denegar el ejercicio de tales derechos «cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras» (93). Esto supone que se concede a la autoridad administrativa el decidir sobre el contenido esencial de un derecho fundamental desde una posición de absoluta supremacía, sin necesidad de atenerse a más razones que esas referencias genéricas. Suscribimos la posición de Lucas Murillo, para quien esa falta de concreción que da por buena la denegación del ejercicio de los derechos de defensa, por ejemplo, frente a datos inexactos, incompletos, ilícitamente obtenidos o absolutamente erróneos, y que no admite formas de acceso parcial o indirecto (por ejemplo, a través de la Agencia de Protección de Datos), incurre en desproporción y genera una disminución de las garantías de las personas (94). En consecuencia, también aquí planea la sombra de inconstitucionalidad.

En sexto lugar, los ficheros de las fuerzas y cuerpos de seguridad tienen un régimen jurídico especialmente lesivo de la intimidad informática. De una parte, se vulnera el principio del consentimiento de los afectados. La LORTAD dispone que la recogida y tratamiento informatizado para «fines policiales» de datos personales «sin consentimiento» de los afectados «están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad» (95). Esta cláusula mantiene relación con el Convenio de Schengen.

Además, una confusa y problemática disposición de la LORTAD establece que la recogida y tratamiento de datos sensibles «podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta» (96). Lucas Murillo ha formulado una hábil interpretación del precepto citado (art. 20.3 LORTAD), conforme a la cual, al no contar con una cláusula expresa excluyendo la necesidad de consentimiento, como la contenida en el art. 20.2 LORTAD, exige recabar tal consentimiento a falta de una específica autorización legal o judicial (97). La tesis de este autor implica, en definitiva, reconducir la cues-

(92) LUCAS MURILLO: *Informática...*, págs. 102-103.
(93) Art. 21.2 LORTAD.
(94) LUCAS MURILLO: *Informática...*, pág. 104.
(95) Art. 20.2 LORTAD.
(96) Art. 20.3 LORTAD.
(97) LUCAS MURILLO: *Informática...*, pág. 108.

tión de los datos sensibles al planteamiento general que efectúa el art. 7 LORTAD. Ahora bien, si el art. 20.3 LORTAD no establece una *lex specialis* sobre los datos sensibles, distinta a la que dispone la *lex generalis* del art. 7 LORTAD, ¿qué sentido tiene? Sólo caben, a mi juicio, dos respuestas posibles que conducen, prácticamente, a la misma conclusión. O bien, en primer lugar, se estima que el art. 20.3 LORTAD establece un régimen específico sobre los datos sensibles excluyendo la necesidad de consentimiento para que los recaben las fuerzas policiales, en cuyo caso me parece inconstitucional y debería desaparecer; o bien se trata de un precepto superfluo, pues repite el art. 7 LORTAD, en cuyo caso debiera también desaparecer siquiera fuese por elegancia legislativa.

Si ante los ficheros de las fuerzas policiales, de una parte, se produce una quiebra del principio del consentimiento, de otra, también se genera otra lesión a la intimidad informática al establecerse que los responsables de tales ficheros «podrán denegar el acceso, la rectificación o la cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando» (98). Esta disposición ha sido severamente criticada por conceder a los responsables de los ficheros un margen de discrecionalidad amplísimo, desproporcionado y donde se echan en falta controles efectivos, pues ni siquiera se contempla una forma de acceso indirecto, aunque fuese parcial, a través de la Agencia de Protección de Datos que permitiera por esa vía conseguir alguna rectificación o cancelación de datos.

b.II. La normativa sobre el SIS presenta diversos aspectos problemáticos. En primer lugar, excluye de forma clara el principio del consentimiento. El presupuesto que anima todo el SIS es la posibilidad de almacenar una serie de datos, alguno de ellos de carácter potencialmente sensible (99), sin contar con el consentimiento de los afectados (100). Pero no es ésta, con ser importante, la única limitación a la intimidad informática.

En segundo lugar, el SIS aparentemente garantiza el principio de calidad de los datos, en cuanto exige que éstos sólo sean utilizables para *cada una* de las finalidades con las que se recogieron (para identificar personas buscadas para su detención, extranjeros no admisibles, personas desaparecidas o testigos) (101). Ahora bien, se

(98) Art. 21.1 LORTAD.

(99) El art. 94.3 del Convenio de Schengen establece qué tipo de datos pueden ser tratados por el SIS. Entre ellos, en su apartado *b)* alude a «los rasgos físicos particulares, objetivos e inalterables». Esta cláusula es potencialmente peligrosísima y puede afectar a datos muy sensibles. El genoma humano es, sin duda, un rasgo físico «particular, objetivo e inalterable», por lo que, en principio, podría ser tratado por el SIS. Ahora bien, no cabe duda de que el genoma es lo absolutamente íntimo del ser humano en su dimensión física y, precisamente por ello, su conocimiento o su tratamiento sin consentimiento del interesado resulta *totalmente* inaceptable.

(100) Las personas cuyos datos pueden ser tratados por el SIS, en virtud del Convenio de Schengen, son: las personas buscadas para su detención (art. 95), los extranjeros que estén incluidos en la lista de no admisibles (art. 96), las personas desaparecidas (art. 97), los testigos en juicio (art. 98).

(101) Art. 102.1 en relación con los arts. 95 a 98 del Convenio de Schengen.

admite una excepción. Es posible que los datos obtenidos para una de las finalidades perseguidas puedan ser utilizados para otra en función de «la necesidad de prevenir una amenaza grave inminente para el orden y la seguridad públicos, por razones graves de seguridad del Estado o con vistas a prevenir un hecho delictivo grave», si bien será necesario contar con «la autorización previa» (102) de la parte contratante informadora» pero nunca del afectado.

En tercer lugar, en principio se reconoce el derecho de toda persona a acceder a los datos que se refieran a ella y estén introducidos en el SIS, de acuerdo con lo que prevea (también en orden a restringir ese derecho) la normativa nacional. Ahora bien, «no se facilitará información a la persona de que se trate si dicha información pudiera ser perjudicial para la ejecución de la tarea legal consignada en la descripción (de los datos) o para la protección de los derechos y libertades de terceros». También se denegará el acceso «en todos los casos durante el período de descripción con vistas a una vigilancia discreta» (103).

En cuarto lugar, se reconocen los derechos a rectificar errores de hecho o de derecho que se refieran a la persona afectada (104) y a la tutela judicial en materia de rectificación, supresión, información o indemnización por las descripciones efectuadas de la persona (105). Además, se establece un plazo máximo de tres años para examinar la necesidad de conservar los datos de suerte que a falta de *necesidad* (no de conveniencia, sino de necesidad) procederá la cancelación de los datos (106).

En quinto lugar, un elemento esencial del SIS es la posibilidad de cesión y transmisión de los datos personales entre los Estados miembros del mismo. Ciertamente, en lo relativo a la cesión de los datos, se proclaman los principios de lealtad, exactitud, rectificación, cancelación y responsabilidad (107), así como la exigencia de que el Estado destinatario garantice para el uso de los datos transmitidos un nivel de protección al menos igual al que esté previsto en su Derecho para la utilización de los datos de carácter similar (108). Sin embargo, existe una grave excepción. Aunque se dice que «los datos únicamente podrán ser transmitidos a los servicios y autoridades de policía», también se abre la puerta a «la comunicación de los datos a otros servicios» (¿Hacienda?), lo que sólo podrá tener lugar «previa autorización de la Parte contratante que los proporcione» (109) (¡pero no de la persona afectada!).

(102) Art. 102.3 del Convenio de Schengen.
(103) Art. 109 del Convenio de Schengen.
(104) Art. 110 del Convenio de Schengen.
(105) Art. 111 del Convenio de Schengen.
(106) Art. 112 del Convenio de Schengen.
(107) Arts. 126 y 129.a del Convenio de Schengen.
(108) Art. 127.2.b del Convenio de Schengen.
(109) Art. 129.2.b del Convenio de Schengen.

2) *Particulares*

Una dimensión importante en que juega la Drittwirkung con carácter general es el de la informática. La doctrina ha reclamado la necesidad de una regulación de la informática que abarque tanto al Estado como a las empresas privadas acerca de los datos que puede llegar a manejar cualquiera de ellos en el tráfico comercial, laboral o administrativo (110). Este aspecto ha sido recogido por la normativa vigente.

La LORTAD, con carácter general, es también de aplicación a los datos personales que figuren en ficheros automatizados del sector privado (111). Ahora bien, existe una importante excepción a esta regla: los ficheros mantenidos por «los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros». La excepción no es absoluta, pues la cesión de dichos datos se somete a las normas correspondientes de la LORTAD (art. 11), salvo que se trate de datos «sensibles», en cuyo caso rigen las prohibiciones del art. 7 (112).

En las relaciones entre particulares rigen los mismos principios y derechos que rigen en las relaciones entre los poderes públicos y el titular del derecho a la intimidad informática (113). No obstante, afortunadamente, no se trasladan a las relaciones entre particulares las numerosísimas exclusiones de la eficacia del derecho que se contemplaban en la relación del particular con los poderes públicos, lo que ha hecho decir a algún autor que en los ficheros de titularidad privada se garantiza una «defensa teórica de la intimidad personal y familiar», de tal suerte que la protección de los datos personales «parece» completa (114).

Sin embargo, hay dos aspectos que, a mi modesto entender, se hallan muy insuficientemente regulados. En primer lugar, la ley dispone que «no será preciso el consentimiento» para el tratamiento automatizado de los datos personales «cuando se refieran a personas vinculadas por una relación negocial, una relación laboral... o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato» (115). Ciertamente, de este precepto están excluidos los datos «sensibles» (ideología, religión, creencias, origen racial, salud y vida sexual). Ahora bien, en todo lo demás, es posible que un sujeto privado con carácter de empleador o una compañía de seguros puedan acopiar, sin consentimiento del afectado con el que mantienen una relación contractual, todos los demás datos personales, alegando que son «necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato».

---

(110) MADRID CONESA: *op. cit.*, págs. 78 y sigs.

(111) Art. 2.1 LORTAD.

(112) Art. 2.2.e LORTAD.

(113) Vid. *supra*, cap. IV.2, págs. 15 y sigs.

(114) MIGUEL ANGEL DAVARA RODRÍGUEZ: «La ley española de protección de datos (LORTAD): ¿una limitación al uso de la informática para garantizar la intimidad? (y II)», en *Actualidad Informática Aranzadi*, 19 de noviembre de 1992, págs. 1 y sigs., págs. 3 y 4.

(115) Art. 6.2 LORTAD.

En segundo lugar, el responsable de un fichero privado no tiene el deber de informar al afectado de la primera cesión de datos que haya efectuado «cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso, sólo será legítima en cuanto se limite a la finalidad que la justifique» (116). En los casos de empleadores o de compañías de seguros es fácil alegar que el «desarrollo, cumplimiento y control» de la relación jurídica implica la conexión de sus ficheros con los de terceros, en cuyo caso puede procederse a la cesión de datos personales no «sensibles» (117) sin consentimiento.

V. LAS GARANTIAS

A. *Institucionales. La Agencia de Protección de Datos*

1. Como advierte Pérez Luño, entre las ventajas que ofrece el sistema del *Ombudsman* para la protección efectiva de los derechos fundamentales pueden citarse, en primer lugar, su función dinamizadora, adaptadora y de reciclaje de los derechos, realizada básicamente a través de los informes periódicos presentados ante los Parlamentos de los que son comisionados; en segundo lugar, su función orientadora de los ciudadanos, agilizando y clarificando los procedimientos de tutela de las libertades, y en tercer lugar, la función preventiva de las agresiones a los derechos, evitando agresiones y daños de difícil o imposible reparación, ya que al ejercicio de las libertades es de cabal aplicación el principio *melius est prevenire quam reprimere* (118).

Las ventajas del *Ombudsman* general en la defensa de los derechos fundamentales generales se multiplican al encontrarnos ante lo que ha llamado Fairén los «*Ombudsman* especiales» que se pueden distinguir del *Ombudsman* puro, bien porque no son nombrados por el Parlamento, sino por otro órgano (Gobierno, Rey...), bien porque son supervisores sólo de determinados campos de acción (actuaciones anti-trust, defensa de los consumidores...) y no de la defensa de los derechos fundamentales en general o bien por ambas razones (119).

En esta categoría pudieran clasificarse los comisarios encargados de la protección de datos personales, que se encargan de supervisar un campo de acción muy concreto: el referido al derecho a la intimidad en el terreno de la informá-

(116) Arts. 25.2 y 11.2.c LORTAD.

(117) El art. 7.3 LORTAD sólo permite la cesión «cuando por razones de interés general así lo disponga una ley o el afectado consienta expresamente».

(118) ANTONIO ENRIQUE PÉREZ LUÑO: «Intimidad y protección de datos personales: del *habeas corpus* al *habeas data*», en SAN MIGUEL: *op. cit.*, págs. 36 y sigs., pág. 43.

(119) VÍCTOR FAIRÉN GUILLÉN: «El Ombudsman y sus posibilidades en España y países iberoamericanos», en íd.: *Temas del ordenamiento procesal*, tomo III, Madrid, Tecnos, 1982, págs. 1505 y sigs., págs. 1532-1533.

tica. Este tipo de órganos o instituciones puede ser unipersonal o colegiado, estar nombrado por el Parlamento o por el Ejecutivo, si bien es claro que el no depender del Ejecutivo —que es uno de los principales, si no el principal, agente amenazante (y lesivo) de ese derecho— parece garantía de que podrá controlar con mayor independencia a ese mismo Ejecutivo. Numerosos países recogen figuras de este tipo (Canadá, Suecia, Noruega, Dinamarca, Francia, Gran Bretaña y Alemania).

2. En España, la protección institucional general de los datos personales no se ha encomendado al Defensor del Pueblo. La razón es que se temía desnaturalizar a esta institución si se ampliaba su campo de actuación de las administraciones públicas a los sujetos privados (120). De ahí la creación *ex novo* de un órgano específico, sin menoscabo de las competencias del Defensor del Pueblo y de los órganos análogos de las CC.AA., la Agencia de Protección de Datos. Esta Agencia es el «*Ombudsman* especial» para la protección del derecho a la intimidad informática y se halla regulada por la LORTAD y por su propio Estatuto (121). La Agencia es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones (122).

2.a. La Agencia se estructura en un Director, un Consejo Consultivo, un Registro General de Protección de Datos y la Secretaría General (123). El verdadero eje de la Agencia es su *Director*. Este, que tiene la consideración de alto cargo, es nombrado por el Gobierno, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años. Aunque la ley prescribe que ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas, lo cierto es que puede ser separado de su cargo por el Gobierno, oídos los restantes miembros del Consejo Consultivo, «por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito de doloso» (124). Esta normativa, aunque parece circunscribir mucho la posibilidad de cese anticipado, no es suficiente para impedir la instrumentalización gubernamental para desembarazarse de una persona molesta para el Poder Ejecutivo (125). En todo caso, dado que, de un lado, las causas de cese están tasadas y, por tanto, el Director no puede ser separado libremente por el Gobierno, y de otro, la Constitución proclama el Estado de Derecho (art. 1.1 CE) y el derecho a acceder a cargos públicos (art. 23.2 CE), estimo que el cese anticipado del Director de la Agencia es recurrible ante los Tribunales Contencioso-Administrativos y aun ante el Tribunal Constitucional por la vía del recurso de amparo.

---

(120) PÉREZ LUÑO: *Derechos humanos...*, cit., pág. 372.

(121) Arts. 34 y sigs. LORTAD; RD 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (EAPD).

(122) Art. 34.2 LORTAD.

(123) Art. 11 EAPD.

(124) Art. 35 LORTAD.

(125) LUCAS MURILLO: *Informática...*, pág. 125.

El *Consejo Consultivo* es un órgano de asesoramiento del Director que emitirá informe en todas las cuestiones que le someta el Director y podrá formular propuestas en temas relacionados con las materias de competencia de la Agencia. El Consejo se compone de nueve miembros nombrados por diferentes instituciones (126), las cuales podrán cesarlos (127).

El *Registro General de Protección de Datos* es el órgano de la Agencia al que corresponde velar por la publicidad de la existencia de los ficheros automatizados de datos personales con miras a hacer posible los derechos de información, acceso, rectificación y cancelación de datos previstos en la LORTAD (128).

La *Inspección de Datos* es el órgano de la Agencia al que competen las funciones inherentes al ejercicio de la potestad de inspección que el art. 39 LORTAD atribuye a la Agencia (129).

La *Secretaría General*, finalmente, desarrolla diversas funciones, entre las que se halla elaborar los informes y propuestas que le solicite el Director (130).

2.b. La LORTAD asigna importantes funciones a la Agencia. Entre otras, merecen destacarse las siguientes: velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos; atender las peticiones y reclamaciones formuladas por las personas afectadas; proporcionar información a las personas acerca de sus derechos en materia de tratamiento automatizado de los datos de carácter personal: ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros, cuando no se ajusten a las disposiciones de la ley; informar, con carácter preceptivo, los proyectos de disposiciones generales de desarrollo de la LORTAD y cualesquiera proyectos de ley o reglamento que incidan en la materia propia de la citada LORTAD, y velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico (131).

Además de las anteriores, la Agencia podrá inspeccionar los ficheros a los que se refiere la LORTAD recabando cuantas informaciones precise para el cumplimiento de sus cometidos. A tal efecto, el responsable del fichero estará obligado a permitir el acceso a los locales en los que se hallen los ficheros y los equipos informáticos previa exhibición por el funcionario actuante de la autorización expedida por el Director de la Agencia. Cuando dichos locales tengan la consideración cons-

(126) Congreso de los Diputados, Senado, Administración General del Estado, CC.AA., Administración Local, Real Academia de la Historia, Consejo de Universidades, Consejo de Consumidores y Usuarios, Consejo Superior de Cámaras de Comercio, Industria y Navegación.

(127) Art. 37 LORTAD; arts. 19 y 20.2.d EAPD.

(128) Art. 23 EAPD.

(129) Art. 27.1 EAPD.

(130) Art. 30 EAPD.

(131) Art. 36 LORTAD; arts. 4-6 EAPD.

titucional de domicilio, la labor inspectora deberá ajustarse además a las reglas que garantizan su inviolabilidad (132).

3. El Convenio de Schengen también establece garantías de tipo institucional. De una parte, obliga a que cada parte contratante designe a una autoridad de control que, respetando el Derecho nacional, se encargue de ejercer un control independiente sobre el fichero de la parte nacional del SIS y de comprobar que el tratamiento y la utilización de los datos introducidos en el SIS no atentan contra los derechos de la persona de que se trate. A tal fin, la autoridad de control tendrá acceso al fichero de la parte nacional del SIS. Por lo demás, se reconoce el derecho de toda persona a solicitar a las autoridades nacionales de control que comprueben los datos referentes a ella integrados en el SIS, así como el uso que se haga de dichos datos (133). Parece claro que la autoridad nacional de control del SIS en España es la Agencia de Protección de Datos.

De otra parte, también se crea una «autoridad de control común» encargada del control de la unidad de apoyo técnico del SIS que pone en conexión las partes nacionales del mismo. Esta autoridad se compone por dos representantes de cada autoridad nacional de control. En su seno, cada parte contratante dispondrá de un voto deliberativo. El control que lleve a cabo esta autoridad se ejercerá «de conformidad» con lo dispuesto en el Convenio de Schengen, en el Convenio 108 del Consejo de Europa y «teniendo en cuenta» la Recomendación R (87) 15, de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa, dirigida a regular la utilización de datos de carácter personal en el sector de la policía y con arreglo al Derecho nacional de la parte contratante responsable de la unidad de apoyo técnico. Además, la autoridad común tendrá competencia para analizar las dificultades de aplicación o de interpretación que pudieran surgir con motivo de la explotación del SIS para estudiar los problemas que pudieran plantearse ora en el ejercicio del control independiente efectuado por las autoridades de control nacionales de las partes contratantes, ora en el ejercicio del derecho de acceso al sistema, amén de elaborar propuestas armonizadas con vistas a hallar soluciones comunes a los problemas existentes. Los informes que emita la autoridad común en el ejercicio de sus competencias serán remitidos a los organismos a los cuales las autoridades de control nacional remitan sus informes (134).

B. *Penales*

Romeo ha afirmado que un breve examen de la protección penal de la intimidad en nuestro Derecho revela que aquélla responde a concepciones ya superadas y parcelarias, que resulta insuficiente, y, por tanto, insatisfactoria, y mucho más si la vulneración se produce por medios informáticos (135).

---

(132) Art. 39 LORTAD; art. 28 EAPD.

(133) Art. 114 del Convenio de Schengen.

(134) Art. 115 del Convenio de Schengen.

(135) CARLOS MARÍA ROMEO CASABONA: *Poder informático y seguridad jurídica*, Madrid, Fundesco, 1987, pág. 24.

1. El art. 192 bis CP introducido por la LO 7/1984, de 15 de octubre, sanciona a la «autoridad, funcionario público o agente de éstos que sin la debida autorización judicial, salvo, en su caso, lo previsto legalmente en desarrollo del art. 55.2 de la Constitución, interceptare las comunicaciones telefónicas o utilizare técnicas de escucha, transmisión, grabación o reproducción del sonido», siendo aplicable la pena inmediatamente superior en grado si divulgare o revelare la información así contenida. Se colma así una laguna, pues anteriormente estas conductas eran atípicas, quedando la intimidad desprotegida en este importante sector.

Romeo ha sostenido, frente a los primeros comentaristas del nuevo precepto que piensan que lo que se protege es la intimidad de las comunicaciones exclusivamente orales, que sería posible entender incluida en este delito la interceptación ilegal de datos informáticos de una persona que afecten a su intimidad y que sean transmitidas por medio telefónico, pues tanto el art. 192 bis CP como el 497 bis CP sólo dicen «interceptare sus comunicaciones telefónicas», y éstas pueden ser orales, informáticas o visuales o de fax (136).

2. El art. 497 bis CP, introducido al mismo tiempo que el art. 192.bis, ofrece una protección inequívoca de las comunicaciones telefónicas frente a las acciones de los particulares. Dicho artículo establece que quien para descubrir los secretos o la intimidad de otros sin su consentimiento interceptare sus comunicaciones telefónicas o utilizare instrumentos o artificios técnicos de escucha, transmisión, grabación o reproducción del sonido será castigado con pena de arresto mayor y multa. Estas penas se agravarían si el autor divulgare o revelare lo descubierto. Todo lo dicho respecto al art. 192 bis CP es aplicable aquí.

3. Si bien con los preceptos introducidos en 1984 la situación ha mejorado, como afirma Romeo, los artículos del Código Penal español dedicados al descubrimiento y revelación de secretos (arts. 497 y sigs. CP), que afectan en gran medida a la intimidad individual, abarcan a duras penas algunas de las modalidades específicas de atentados a la intimidad con medios informáticos. La LORTAD ha sido otra oportunidad perdida para tipificar penalmente las acciones que lesionan la intimidad informática.

C. *Administrativas*

1. La vulneración por los poderes públicos o por los particulares del derecho a la intimidad informática puede constituir una infracción leve, grave o muy grave. Son infracciones leves, entre otras, el no proceder de oficio o a instancia de parte a rectificar o cancelar los errores, lagunas o inexactitudes formales de los ficheros, así como no mantener éstos actualizados (137).

Entre las infracciones que se consideran graves se encuentran las siguientes:

(136) ROMEO: *op. cit.*, pág. 29.
(137) Art. 43.2.b-c LORTAD.

crear ficheros públicos de datos personales sin autorización de disposición general; crear ficheros privados de datos personales con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad; recoger datos personales sin consentimiento expreso de los afectados, cuando éste sea exigible, o sin proporcionarles la pertinente información; tratar los datos personales con conculcación de los principios y garantías de la LORTAD; no efectuar rectificaciones o cancelaciones de datos cuando resulten afectados los derechos de las personas amparadas por la LORTAD; vulnerar el deber de secreto si no afecta a datos «sensibles»; mantener los ficheros y equipos sin las debidas condiciones de seguridad (138).

Por último, se consideran muy graves las siguiente infracciones: la recogida de datos en forma fraudulenta y engañosa; la cesión de datos en los casos no permitidos por la ley; tratar datos «sensibles» sin consentimietno expreso del afectado o sin que un ley lo disponga; no cesar en el uso ilegítimo de los tratamientos automatizados de datos personales cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por los titulares del derecho de acceso; la transferencia, sin autorización del Director de la Agencia, de datos personales a países que no proporcionen un nivel de protección equiparable al español; el tratamiento de datos personales de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales y la vulneración del deber de guardar secreto sobre los datos personales «sensibles» (139).

2. Las infracciones muy graves prescriben a los tres años, las graves a los dos años y las leves al año (140). Estas últimas se sancionan con multas de 100.000 a 10 millones de pesetas; las graves, con multas de 10 millones y una pesetas a 50 millones de pesetas, y las muy graves, con multas de 50 millones y una pesetas a 100 millones de pesetas. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad y a la reincidencia (141).

Por lo demás, en los supuestos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de los ficheros, públicos o privados, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas (142).

(138) Art. 43.3 LORTAD.
(139) Art. 43.4 LORTAD.
(140) Art. 46.1 LORTAD.
(141) Art. 44 LORTAD.
(142) Art. 48 LORTAD.

3. El Convenio de Schengen no establece sanciones disciplinarias por el abuso en la utilización de los datos, pero establece que 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 SIS. Lo mismo ocurrirá cuando los daños hayan sido causados por la parte contratante informadora si ésta hubiere introducido datos que contengan errores de hecho o de derecho. Además, se establece que si el Estado contra el que se emprenda una de estas acciones no fuera la parte contratante que proporcionó la información, esta última estará obligada a reembolsar, si se le pide, las cantidades pagadas con carácter de indemnización, a no ser que los datos hubieren sido utilizados por la parte contratante requerida incumpliendo el Convenio de Schengen (143).

(143) Art. 116 del Convenio de Schengen.