ANTE LA RATIFICACION DEL CONVENIO DE PROTECCION DE DATOS DEL CONSEJO DE EUROPA

Por MANUEL HEREDERO HIGUERAS

I

Remitido en su día por el Gobierno al Congreso de los Diputados, el «Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal», hecho en Estrasburgo el 28 de enero de 1981 y firmado por España el mismo día del año siguiente, el 2 de noviembre fue dictaminado por la Comisión de Asuntos Exteriores del Congreso y acordada su remisión al Senado. A su vez, la Presidencia del Senado en igual fecha acordó enviar a la Comisión de Asuntos Exteriores del Senado y publicar en el *Boletín Oficial de las Cortes Generales* (Senado), a los efectos previstos en el artículo 131-1 del Reglamento de dicha Cámara, el citado Convenio. El plazo de presentación de enmiendas transcurrió sin que se formulara enmienda alguna. En consecuencia, con fecha 22 de diciembre el Senado acordó conceder al Gobierno la autorización para ratificar, prevista

en el artículo 94-1 de la Constitución. Es oportuno formular algunas consideraciones acerca de las consecuencias de dicha autorización, en relación con el mandato del artículo 18-4 de la Constitución.

Los Estados que hasta ahora han ratificado el Convenio —Suecia y Francia— disponen de una legislación interna que da cumplimiento al Convenio en el ámbito del Derecho interno. No es éste el caso del Estado español, pues las dispersas disposiciones, de rango reglamentario todas ellas, actualmente en vigor, no permiten construir un Derecho positivo interno suficiente. Tales disposiciones son la Orden de la Presidencia del Gobierno de 13 de diciembre de 1978, reguladora del uso del archivo de datos del Centro de Investigaciones Sociológicas; la Orden del que fue Ministerio de Sanidad y Seguridad Social de 24 de octubre de 1978 por la que se creaba la Cartilla Sanitaria de la Embarazada; y la Orden del Ministerio de Hacienda de 30 de julio de 1982 sobre seguridad de las bases de datos fiscales. Cabría añadir el artículo 14-2 del texto refundido de la Ley de Seguridad Social aprobado por Decreto 2065/1974 vigente en la parte que resulta del Real Decreto 26/1978; este precepto contiene una formulación del derecho de acceso, pieza central de la normativa del Convenio y de las legislaciones nacionales. De ahí que no sea posible que el Convenio, una vez ratificado, sea *self-executing*. Un caso parecido es el de Italia, que dispone de una regulación de ficheros de datos personales, pero limitada a los ficheros policiales. La Ley número 121, de 1 de abril de 1981 relativa a la organización de la Administración de la Seguridad Nacional, contiene seis artículos al respecto. Una tal regulación sectorial es insuficiente para dar cumplimiento al Convenio. La ratificación llevaría, pues, aparejada la exigencia de disponer de una legislación interna dentro de un plazo determinado. Dicho plazo es de cuatro meses a partir de la fecha en que el Convenio entrare en vigor con respecto a España (arts. 4-2 y 22-2 del Convenio). Si España fuera el tercero de los Estados que ratificaren el Convenio, la legislación interna española deberá estar en vigor «el primer día del mes subsiguiente a la expiración del plazo de tres meses que siguiere a la fecha» en la cual el quinto de los Estados miembros del Consejo de Europa hubiere depositado el instrumento de ratificación, adhesión o aprobación en poder del secretario general del Consejo de Europa. Es decir, cuatro meses, como máximo, desde la última de las cinco ratificaciones previstas para la entrada en vigor del Convenio con carácter general.

En rigor, de acuerdo con el Derecho vigente, constituido por el artículo 94-1 de la Constitución, el Convenio de Viena sobre el Dere-

cho de los Tratados, y el artículo 1-5 del Código Civil, el Convenio ha de pasar los trámites siguientes una vez firmado:

a) Autorización al Estado, por el Congreso y el Senado, para manifestar el consentimiento del Estado para obligarse por el tratado; esta autorización *no implica una obligación de ratificar*, ni, por consiguiente, la expresión del consentimiento está sujeta a plazo.

b) Entrega del instrumento de ratificación al secretario general del Consejo de Europa; tampoco está sujeto a plazo.

c) Publicación del texto del instrumento de ratificación en el *Boletín Oficial del Estado*.

Lo exiguo del plazo previsto en el Convenio para que el Estado español lo ejecute mediante una ley interna obliga a diferir la evacuación de los dos últimos trámites en función del ritmo del procedimiento de aprobación de la ley de protección de datos. Es decir, una vez autorizada la ratificación, ésta puede diferirse hasta tanto sea racionalmente previsible que la ley será aprobada por el Senado en un plazo inferior a tres meses.

II

Sin perjuicio del margen de maniobra que los distintos trámites del procedimiento de autorización y ratificación permitan, en cuanto a la fecha efectiva de entrada en vigor del convenio, su ratificación tendrá como consecuencia principal agregar al mandato del artículo 18-4 de la Constitución un nuevo mandato que reforzará el primero y fijará un plazo para su ejecución. Pero por otra parte el Convenio ratificado no será solamente un refuerzo para el artículo 18-4 de la Constitución, sino que a la vez perfilará y aclarará el alcance de este precepto. En rigor, dicho alcance no debía ofrecer dudas pese a su poco afortunada redacción, sobre todo si se tiene en cuenta la discusión parlamentaria del Anteproyecto de Constitución.

Es escasa la atención que la doctrina ha dedicado a este precepto. Sólo se encuentra un análisis detallado en los comentarios de Oscar Alzaga. El profesor Alzaga considera que el precepto es superfluo, por cuanto que no hace otra cosa que definir un supuesto más de atentado contra la intimidad, el honor y los derechos y libertades, que viene a añadirse a los supuestos generales susceptibles de ser encuadrados en la dicción del artículo 18-1. Contemplado así el apartado 4 del artículo 18 sólo prevé los atentados a la intimidad, etc., cometidos por medio de la

informática. Evidentemente, visto así el precepto resulta absurdo que contenga una verdadera reserva de la ley orgánica para un supuesto específico de los contemplados en el apartado 1. La discusión parlamentaria permite, sin embargo, llegar a una conclusión distinta. Abundando en la misma idea del profesor Alzaga, el señor Sancho Rof propuso la supresión del apartado 4 del (entonces) artículo 17 del anteproyecto, mediante la enmienda 716. Sin embargo, hubo otras dos enmiendas, la 470, formulada por el Grupo Mixto, y la 117, de la minoría catalana, suscritas respectivamente por Raúl Morodo y Miguel Roca Junyent. La primera proponía un texto diferente, según el cual:

> la ley regulará el acopio, uso y difusión de los datos personales contenidos en los archivos o registros susceptibles de acceso automático, con objeto de garantizar las libertades públicas y el ordenamiento constitucional.

En este texto se contenía en forma sintética la problemática de las leyes europeas de protección de datos. Sin embargo, la comisión, aun admitiendo que el texto propuesto no era más que una especie de perífrasis extensa de la noción de informática, no la aceptó. No obstante, la defensa de la enmienda 117 por los diputados Roca Junyent, Martín Toval y Solé Tura mostró cuál era a juicio de los mismos el alcance exacto del precepto. Las intervenciones de estos diputados mostraron que conocían la problemática exacta implicada, como se infiere de sus alusiones a problemas reales suscitados en Francia y otros países. No obstante, lo único que se logró fue añadir a la dicción del precepto de referencia al libre ejercicio de los derechos y libertades reconocidos en la Constitución, a modo de ampliación de los bienes jurídicos cuya defensa requiere, a juicio del legislador constituyente, la limitación del uso de la informática.

A pesar de esta coincidencia sustancial entre la intención del legislador constituyente y la problemática de la protección jurídica de los datos personales, la dicción del artículo 18-4 sigue dando pie a la interpretación a que se aludió anteriormente. La ratificación del Convenio del Consejo de Europa introducirá un mandato adicional, pero cuyos téminos no ofrecen duda. Basta con examinar el artículo primero, que define el fin y objeto del Convenio:

> garantizar ... a toda persona física, cualesquiera que fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales y en especial de su derecho a la intimidad, con relación al tratamiento automático de los datos de carácter personal que le concernieren.

El artículo 4 precisa las obligaciones que contrae el Estado parte en el Convenio. Se trata de una regulación del uso de los datos personales de acuerdo con sus principios y unas garantías, reconociendo a las personas unos medios para hacer valer tales principios y garantías. No es, pues, una *ley informática*, que hubiera de regular los diversos aspectos en que la informática suscita la necesidad de una disciplina jurídica. Una tal ley sería poco defendible, por cuanto que sacaría de su contexto adecuado problemas diversos (enseñanza, contratos informáticos, propiedad intelectual, etc.). No es tampoco una ley de protección de la intimidad frente a la informática. Tampoco se trata de una ley que limite o restrinja el uso de la informática o de los ordenadores. La obligación que el Reino de España contraerá como consecuencia de la ratificación del Convenio no podrá ser cumplida por vía reglamentaria. Es frecuente acudir a este recurso para ejecutar, por ejemplo, los tratados de doble imposición. Pero en el caso de la legislación de protección de datos, la ejecución del Convenio requerirá una ley orgánica. Así se deduce del artículo 81-1 de la Constitución, por cuanto que la materia a regular hace referencia a los derechos y libertades reconocidos por el capítulo 2.° del título I de la Constitución. En lo que sigue se expone lo que, a nuestro juicio, es la problemática específica al respecto.

III

El problema de fondo es resultado de dos factores. En primer lugar, el fenómeno del *fichage*, por usar el vocablo francés. Toda persona figura normalmente, a sabiendas o no, en más de un centenar de registros, ficheros o archivos. Desde el asiento correspondiente del Registro Civil —es conocida la frase según la cual la vida es el lapso comprendido entre dos asientos del Registro Civil— los registros de vacunación obligatoria, los expedientes escolares, los padrones de habitantes, los registros fiscales, las cajas de recluta, las cuentas bancarias, etc., hasta los registros de actos de última voluntad, el número de los ficheros, archivos o registros en que cada persona figura durante su vida puede llegar a ser realmente elevado. Si, además, el interesado se ve precisado a residir en el extranjero por razones de trabajo o profesión, esta residencia da lugar a que sus datos sean inscritos en registros extranjeros (registros de residentes, de clientes de determinados establecimientos, tarjetas de crédito). Y si una persona trabaja para una

empresa multinacional, y reside transitoriamente en países distintos, sus datos podrán figurar en registros de otros tantos países. De este modo, el número de los registros o ficheros que contengan los datos personales de un individuo puede ser ilimitado. La tecnología actual permite el acceso prácticamente instantáneo de muchos registros. El interesado pierde así totalmente el control de la información que acerca de él se halla registrada en múltiples registros de varios o muchos países. El otro factor estriba en el carácter de bien comerciable que hoy tiene la información. La información es un bien susceptible de apropiación, sin que ello implique una exclusividad de la apropiación. Cabe, por tanto, una multiplicidad de personas o entes que pueden disponer de una misma información. La información es, pues, algo que se puede comprar, vender, elaborar, transformar. No es una excepción al respecto la información de carácter personal. En otras palabras: los datos relativos a las personas tienen un valor mercantil. La consecuencia de todo ello es la pérdida por el individuo del control o dominio de su información personal. Esta situación se agrava por el hecho de los múltiples usos que cabe hacer de la información personal. Esta información puede ser tenida en cuenta como base de decisiones que afectan al individuo (peticiones de empleo, por ejemplo). Cualquier error o cualquier valoración indebida que se agregue a los meros datos, puede repercutir desfavorablemente. Asimismo, la inclusión de determinados datos en los registros (raza, confesión religiosa, militancia política o sindical, patrimonio, país o comarca de procedencia, etc.), puede dar lugar a discriminaciones injustas o, como en un pasado todavía reciente, a persecuciones políticas, raciales o religiosas. La variedad de los supuestos posibles de indefensión del individuo frente a usos indebidos de sus datos personales hace imposible reconducir todos ellos a un único criterio de protección jurídica sustantiva.

El concepto de datos personales cubre una gama variable de informaciones. Desde un conjunto mínimo constituido por la filiación, fecha de nacimiento y domicilio, hasta la totalidad de los datos que resultarían de agregar a este conjunto mínimo los datos de cuentas bancarias, datos de crédito, bienes, rentas, datos profesionales, enfermedades padecidas, etc. El caso extremo sería el conjunto de los datos registrados en los distintos ficheros en que normalmente toda persona está inscrita a lo largo de su vida. No todos los datos tienen que referirse a cualidades personales, sino que pueden referirse asimismo a bienes de los cuales el interesado es propietario (vivienda, embarcacio-

nes, vehículo). Los datos pesonales no son sensibles o vulnerables *per se*, sino sólo según el contexto dentro del cual se usan. Los posibles contextos son múltiples, por lo cual la forma más adecuada de la protección jurídica sería la de carácter preventivo. Sería imposible tratar de enumerar todos los bienes jurídicos o intereses protegibles y pretender sistematizar las facetas del problema con referencia a los distintos bienes jurídicos (intimidad, libertad, honor, etc.) o intereses implicados. El único criterio posible es la creación de un mecanismo preventivo, impulsado por el Estado y controlado por los interesados mediante el ejercicio de unos derechos instrumentales (derechos de acceso, de rectificación, derecho a exigir un uso de los datos conforme a su finalidad, derecho de cancelación de datos irrelevantes, etc.). Esta sensibilidad de los datos personales en función del uso o contexto implica que si es posible aislar determinados supuestos de uso habrá que determinar si el uso de los datos personales requiere o no una protección preventiva específica. Los supuestos más definidos al respecto son los datos utilizados en un contexto *estadístico*, de *investigación* científica, en un contexto *médico*. Asimismo, el uso de datos personales con fines de publicidad directa y venta por correspondencia requiere unas precauciones especiales.

Los sistemas de información médica merecen un tratamiento especial. La razón estriba en los especiales riesgos que los datos médicos ofrecen. Como consecuencia de la siempre creciente especialización, los médicos se ven obligados a intercambiar datos con otros médicos e incluso con otros profesionales. Pero al mismo tiempo los datos deben ser inaccesibles a otras personas, de tal manera que quede a salvo el secreto médico y la intimidad de los enfermos. Por otra parte, el derecho de acceso a los datos del interesado no siempre es prudente que deba ser ejercido con respecto a los datos médicos; según los casos, puede ser contraproducente para el propio interesado. Por ello, en estos casos el derecho de acceso debe ser ejercido por medio de un médico, pero no directamente.

El uso de los datos personales con fines estadísticos o de investigación científica requiere asimismo un tratamiento específico. Por una parte, es preciso distinguir modalidades diversas de investigación (interna, externa), diferenciar la investigación y la planificación, y matizar con respecto a este uso de los datos la aplicabilidad de los principios generales; viabilidad de la regla de la obtención de datos por medios lícitos y legítimos, la procedencia de que esta modalidad de uso de datos sea supervisada a título preventivo por los órganos de protección

de datos. También se han propuesto reglas específicas, como el respeto a la *propiedad de los datos*, el *consentimiento informado*, etc.

Los datos estadísticos ya habían venido siendo objeto de una protección por vía del anonimato y el secreto estadístico. Sin embargo, la informática ha incidido en ellos igualmente. Un caso claro es el de la ley francesa de Estadística, que dispone que todas las personas nacidas entre el 4 y el 10 de octubre de cada año sean seguidas, a título de muestra, para estudios más profundos, lo cual implica un anonimato menor que en el caso de las demás personas. Muchos estudios estadísticos realizados para determinar, por ejemplo, el mayor o menor grado de procedencia de los militares o funcionarios de una región geográfica dada, han sido objeto de reparos por cuanto que tienden a facilitar la identificación y el encuadramiento de las personas en clases predeterminadas.

Otros aspectos los constituyen el uso de datos personales a efectos de la determinación de la solvencia comercial, y el uso de tales datos con fines de publicidad directa y venta por correspondencia. En el caso de la publicidad directa, nos encontramos con el uso del nombre y dirección de una persona sin su consentimiento, y en la mayoría de los casos con una colecta de información realizada por medios de licitud discutible. Cabe, además, la posiblidad de interconectar ficheros, y crear así perfiles de clientes, basados en sus gustos y necesidades, sin que el interesado conozca tales perfiles. Existe, asimismo, en proporción creciente, una actividad publicitaria, la del *corredor de listas*, que adquiere listas que no son del dominio público y las facilita a empresas de publicidad directa. Esta actividad está, en general, al margen de todo control. Las legislaciones que regulan las actividades publicitarias no se ocupan de este problema. Tampoco las legislaciones de protección del consumidor. A escala internacional, existen unas normas deontológicas de la Cámara de Comercio Internacional que establecen unos principios reguladores de la publicidad directa en general y asimismo reconocen un derecho del interesado a saber que está en una lista dada y a exigir que su nombre y dirección sean dados de baja en las listas de la empresa de publicidad directa. Un caso análogo lo constituyen las encuestas o prospecciones de mercados. En éstas es donde puede surgir el problema de los perfiles personales. Es el mismo caso de las encuestas de opinión, encuestas electorales, etc.

El uso de los datos puede ofrecer una dimensión *dinámica*, es decir, los *datos en movimiento*, a través de las fronteras por medio de las redes de transmisión de datos, tales como la red interbancaria SWIFT

(Society for Worldwide Interbank Financial Telecommunications), la SITA (Sociedad Internacional para la Telecomunicación Aeronáutica), las redes de la organización Mundial de Meteorología, las de la INTERPOL. Además de estas redes, por las cuales circulan datos de carácter diverso, en función del ámbito concreto, existen otras por las cuales se transmiten datos de carácter científico, documentación técnica (un caso de éstas es la Red INCA). Asimismo, los medios tradicionales, como el correo o el telégrafo sirven de cauce a esta circulación. Pero en este caso el problema no está limitado a los datos personales. Este uso de los datos ofrece una fisonomía totalmente diferente. En primer lugar, da origen a una dimensión internacional de los problemas del uso de los datos personales, en los casos en que el interesado cambia de residencia, se traslada a otro país por razones profesionales, o cuando empresas multinacionales crean sus ficheros de personal o de clientes y los transfieren de un país a otro. A veces, esta transferencia tiene por objeto evitar la aplicación de leyes de control del uso de datos personales, trasladando los ficheros a países en los cuales no existe tal legislación. Dichos países se denominan a estos efectos, a semejanza de los paraísos fiscales, paraísos de datos *(data havens)*. Este aspecto de la protección de datos requería una solución internacional. El Convenio de Estrasburgo de Protección de Datos responde a esta necesidad. Pero la circulación internacional de datos ha adquirido una dimensión diferente, precisamente en relación con el movimiento de los datos no personales. En un primer momento y cuando aún se contemplaban los problemas del uso de los datos personales *sub specie intimitatis*, se trató de construir un concepto de *intimidad nacional*. Esta idea quedó pronto desbordada y adquirió un carácter político que recoge la dialéctica Norte-Sur, países desarrollados-países en desarrollo.

IV

La solución de estos problemas no puede estar en la adaptación de conceptos o reglas del Derecho privado. No es viable admitir una titularidad dominical o real del interesado sobre sus datos personales. La específica índole de la información en cuanto objeto de derechos y de tráfico jurídico impide reconocer una titularidad exclusiva y no compartida. Aun cuando se pretendiera reconocer una tal titularidad exclusiva, en la práctica no sería viable. Tampoco cabe el recurso al Derecho de obligaciones, concretamente a la culpa extracontractual,

puesto que, a tenor de lo dispuesto en el artículo 1.902 del Código Civil, sería preciso en cada caso probar la producción de un daño, físico o moral. Precisamente se trata de evitar la producción de tal daño. Por otra parte, una vez probada la existencia del daño moral, quedaría abierta la vía de la indemnización de daños y perjuicios y no haría falta una protección específica.

Tampoco hay que insistir en exceso en la protección de la intimidad, del honor, etc., según la dicción del artículo 18-4 de la Constitución. La intimidad no es el único bien jurídico implicado. Hay que entender que la enumeración que a tal respecto se hace en el apartado 4, no es exhaustiva. Además del honor, la intimidad personal y familiar, hay otros bienes jurídicos que deben ser tenidos en cuenta. No es conveniente, por ello, insistir demasiado en la protección de la intimidad o del anonimato de los datos. Tal insistencia puede ser perjudicial para el individuo, por cuanto que puede llegar a impedir la adopción de medidas administrativas que le favorezcan. De ahí que lo que debe ser protegido es la *integridad* de la información personal, en cuanto que es expresión de la *identidad* de la persona. El tráfico incontrolado de la información personal puede dar lugar a distorsiones o alteraciones de la identidad de las personas. El problema no se suscita solamente en la relación Estado-súbdito, en cuanto que el Estado está actualmente en condiciones de adquirir un poder mayor sobre el súbdito al disponer de una información casi total sobre él. Este poder puede adquirirlo, incluso en mayor grado, el particular que compra o vende la información.

La única solución adecuada consiste en la previsión de un mecanismo preventivo, es decir, en dotar al individuo de unos medios jurídicos que le permitan anticiparse al uso indebido de su información personal o evitar la producción de un perjuicio físico o moral. Dicho mecanismo puede consistir en una modalidad de intervención administrativa, en la que un órgano estatal autoriza la llevanza de registros siempre que los responsables de cada registro ofrezcan las garantías necesarias de que el uso de los datos respetará los derechos individuales y las libertades fundamentales. No es imprescindible este mecanismo de intervención administrativa. Cabe la posibilidad de una acción *a posteriori*, es decir, mediante la represión de prácticas contrarias al respeto a los derechos y libertades, por vía de denuncia a un comisario parlamentario, o de actuación de oficio de éste. En ambos supuestos, el sistema se completa con unos derechos *instrumentales*, mediante cuyo ejercicio se ponen en funcionamiento estos mecanismos.

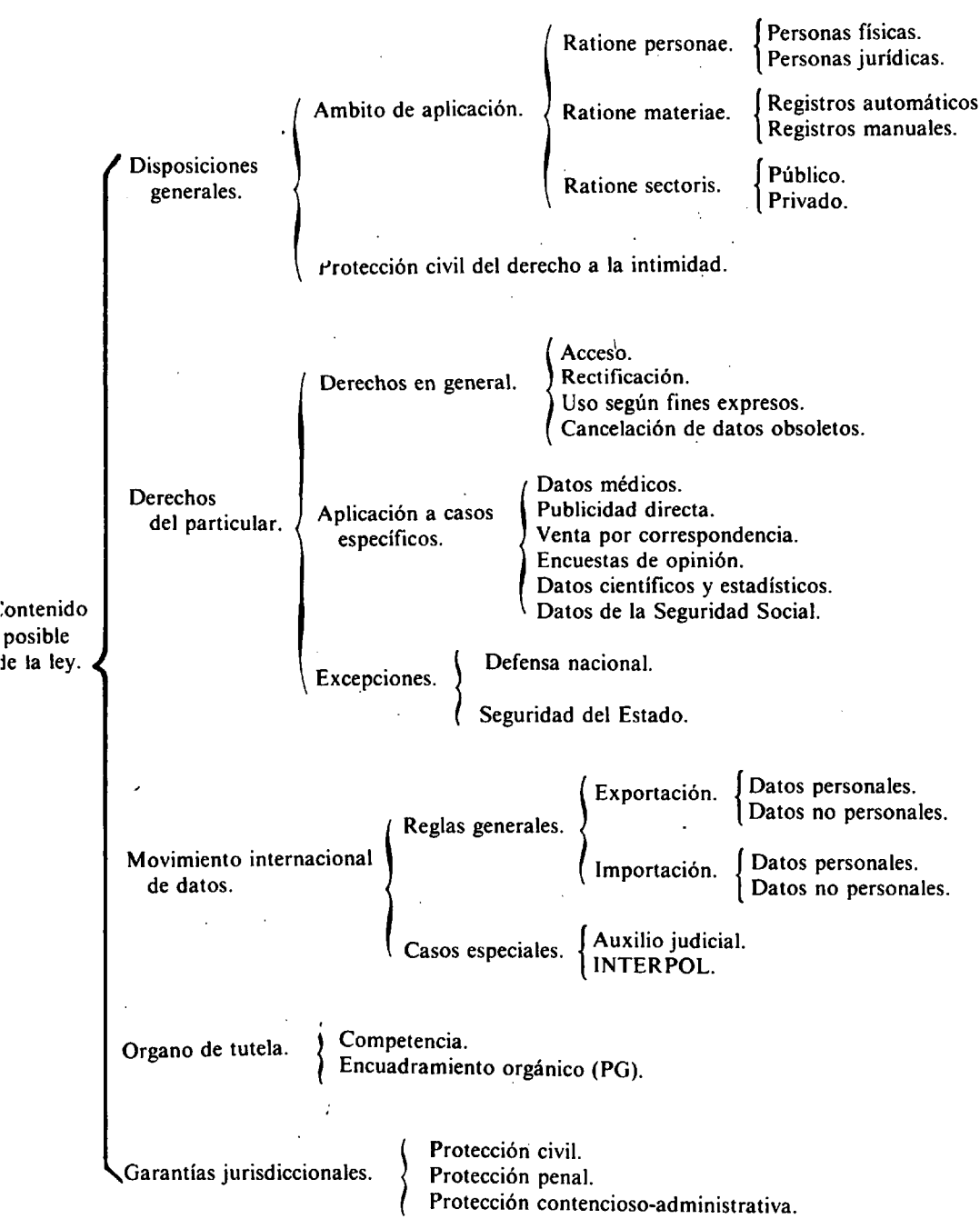
El primero de estos derechos es el denominado *derecho de acceso*. Consiste en el derecho de toda persona a conocer los datos que hay registrados con relación a ella en un fichero dado. El nombre de *derecho de acceso* no debe entenderse en el sentido de derecho a conocer los datos, pero no mediante el acceso automatizado a un soporte de datos. En caso contrario, este derecho se limitaría a los ficheros automatizados, e implicaría la exclusión de los ficheros de consulta manual o convencional. Debido a su paralelismo con la tradicional garantía de *habeas corpus*, se denominó en un principio a este derecho *habeas data* o *habeas scriptum*. Este derecho está reconocido, de un modo u otro, en todas las legislaciones de protección de datos. Su ejercicio no se limita al acceso a los datos a instancia del interesado, sino que puede revestir la forma de una comunicación de tales datos, de oficio, por el responsable del fichero. A este respecto caben tres posibilidades: bien notificar la primera inscripción o anotación, con miras a comprobar la exactitud y completud de los datos; bien notificar periódicamente la existencia de los datos; bien cada vez que se produzca alguna alteración o ampliación de los datos.

Consecuencia del ejercicio del derecho de acceso es el derecho a exigir la *rectificación* o *cancelación* de los datos inexactos o irrelevantes según el fin del fichero. Esto nos lleva a otro de estos derechos: el de exigir que los datos personales sean utilizados de conformidad con el *fin* para el cual fueron incluidos en el fichero. En algunos ordenamientos jurídicos, este derecho impide incluso la interconexión de ficheros de la propia Administración pública. Es el caso de Francia, en la que existe ya jurisprudencia del Consejo de Estado según la cual los datos personales facilitados a la Seguridad Social no pueden ser puestos a disposición de las autoridades policiales, debido a que el administrado los había facilitado para los fines propios de la Seguridad Social. Una aplicación fiel del principio que sirve de base a este derecho es el medio de evitar los problemas que pueden plantearse por el uso de los datos en contextos distintos del previsto: el caso más claro es el de los datos médicos, por ejemplo.

La necesidad de llegar a un cierto equilibrio entre la protección del individuo de una parte, y los intereses del Estado en cuanto al control de la información de otra, exige, sin embargo, prever unas excepciones a las aplicaciones de estos derechos. Tales excepciones hacen referencia a la defensa de la seguridad del Estado, a la seguridad pública, los intereses monetarios del Estado, la represión de los delitos, y son

defendibles sobre la base del Convenio de Roma sobre derechos humanos.

A continuación se incluye un cuadro sinóptico de los temas que podría regular una ley de protección de datos, mediante la cual se ejecutara el aludido doble mandato.


Contenido posible de la ley.
Disposiciones generales.
Ambito de aplicación.
Ratione personae.
Personas físicas.
Personas jurídicas.
Ratione materiae.
Registros automáticos.
Registros manuales.
Ratione sectoris.
Público.
Privado.
Protección civil del derecho a la intimidad.
Derechos del particular.
Derechos en general.
Acceso.
Rectificación.
Uso según fines expresos.
Cancelación de datos obsoletos.
Aplicación a casos específicos.
Datos médicos.
Publicidad directa.
Venta por correspondencia.
Encuestas de opinión.
Datos científicos y estadísticos.
Datos de la Seguridad Social.
Excepciones.
Defensa nacional.
Seguridad del Estado.
Movimiento internacional de datos.
Reglas generales.
Exportación.
Datos personales.
Datos no personales.
Importación.
Datos personales.
Datos no personales.
Casos especiales.
Auxilio judicial.
INTERPOL.
Organo de tutela.
Competencia.
Encuadramiento orgánico (PG).
Garantías jurisdiccionales.
Protección civil.
Protección penal.
Protección contencioso-administrativa.