La situación jurídica internacional y la Ley Orgánica 5/1992

POR **EDUARDO VILARIÑO PINTOS**

Tras revisar la regulación internacional, se concluye que la LORTAD presenta numerosas lagunas y guarda un alto riesgo de inadaptación frente a la futura regulación europea.
Las bases de los derechos de la persona respecto al tratamiento de sus datos personales se encuentran en la Declaración Universal de los Derechos Humanos, en el Pacto Internacional de Derechos Civi- les y Políticos y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

1. INTRODUCCIÓN

La regulación de la protección de la persona respecto a sus datos personales automatizados, viene exigida por la obligación general de protección de los derechos humanos, que resultan particularmente vulnerables, precisamente, en cuanto los datos personales pueden ser tratados a través de las técnicas informáticas.
De ahí que toda regulación de tales datos haya de respetar, como condición irrenunciable para su validez, las disposiciones jurídico-internacionales sobre la protección de los derechos humanos.
Además, en segundo lugar, para su admisibilidad y efectividad, esa regulación ha de conformarse a los instrumentos internacionales que de manera específica regulan o establecen pautas respecto a la protección de datos personales automatizados.
En todo caso, hay que entender que, a pesar de la expresión generalizada «protección de datos personales», el destinatario de la protección es la persona en relación al tratamiento de sus datos personales (desde la obtención hasta su utilización en sentido amplio: elaboración, cesión, transmisión,etc.). Y el alcance de la protección se determinará, en principio, en razón de la transcendencia social o interés social legítimo de esos datos personales.
De esta manera la protección de la persona respecto a sus datos personales se considera como una manifestación de los derechos humanos, dentro del conjunto de los llamados «derechos nuevos» por la Comisión Europea de Derechos Humanos, que se asienta o tiene su fundamento en los principales instrumentos internacionales reguladores de tales derechos.
Así, en cuanto a los instrumentos que afectan a España, hay que señalar:
a) El art. 12 de la Declaración Universal de Derechos Humanos, que prohíbe la injerencia

Fundación Telefónica
Telefónica

arbitraria en la vida privada de las personas, su familia, su domicilio o su correspondencia y los ataques a su honra o a su reputación y establece el derecho de la persona a la protección de la ley contra tales injerencias y ataques.
b) El art. 17 del Pacto Internacional de Derecho Civiles y Políticos, que se manifiesta en los mismos términos que el art. 12 de la Declaración Universal, añadiendo a la prohibición de las injerencias arbitrarias las ilegales.
c) El art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que preceptúa el derecho de toda persona al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. Prohíbe, también, la injerencia de la autoridad pública en el ejercicio de este derecho, cuando no esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y de las libertades de los demás.

2. LOS TEXTOS INTERNACIONALES ESPECÍFICOS SOBRE LA PROTECCIÓN DE LOS DATOS PERSONALES

1. El Proyecto de Principios de las Naciones Unidas
El documento del Consejo Económico y Social de las Naciones Unidas E/CN 4/1990/72, de 20 de febrero «Derechos humanos y desarrollos científicos y técnico», recoge la versión revisada de los principios rectores para la reglamentación de los ficheros informatizados que contienen datos de carácter personal.
Junto a los principios rectores presenta especial interés la facultad de derogación de alguno de ellos a través de la llamada «cláusula humanitaria» que posibilita excluir la prohibición de registrar datos sensibles con el objeto de permitir a las ONG, especializadas en proteger a las personas perseguidas como consecuencia de un trato discriminatorio, basado en el origen racial, la religión, opiniones políticas, etc. Esta cláusula tiene por objeto reconocer como medida necesaria en una sociedad democrática la protección de los derechos y libertades de los demás.
Entre los principios que se proponen en el Proyecto cabe destacar:
– Principio de licitud y de lealtad. La utilización de los ficheros no puede ser contraria a los propósitos y principios de las Naciones Unidas. Los datos no pueden ser obtenidos ni tratados por procedimientos ilícitos o desleales.
– Principio de exactitud. Veracidad de los datos.
– Principio de finalidad. Datos pertinentes a la finalidad perseguida.
– Principio de acceso. El interesado tiene derecho a saber si los datos que se refieren a él son conformes con el objeto del fichero. Cuando se transmitan datos, tiene derecho a conocer los destinatarios. A estos efectos deberá preverse un régimen de recursos ante la autoridad de control.
– Principio de no discriminación. Significa la prohibición de informaciones sensibles cuya utilización pueda engendrar una discriminación ilegítima o arbitraria.
2. Las líneas Directrices de la OCDEE
Consejo de la OCDE aprobó el 23 de septiembre de 1980 una Recomendación relativa a «Líneas directrices sobre protección de la intimidad y de los flujos de datos de carácter personal a través de las fronteras», que constituye, aunque sin obligatoriedad jurídica, el primer instrumento internacional específico en la materia que nos ocupa. Estas Líneas directrices

Fundación Telefónica
Telefónica

consisten en una serie de principios fundamentales que se deben aplicar en el ámbito de las legislaciones internas. Entre ellos:
– Principio de limitación de la colecta de datos. La obtención de datos de carácter personal ha de hacerse por medios legítimos y leales.
– Principio de calidad de los datos. Los datos han de ajustarse a los fines del fichero y deberán ser exactos y completos.
– Principio de especificación del fin. La utilización que se vaya a hacer de los datos debe ser manifestada al obtenerlos.
– Principio de restricción del uso. Como consecuencia de lo anterior, significa que los datos de carácter personal no podrán ser usados para otros fines a no ser que haya consentimiento del interesado o previa habilitación legal al efecto.
– Principio de participación del individuo. Toda persona física deberá gozar de los siguientes derechos: a) Obtener confirmación de si el responsable de datos tiene datos acerca de su persona. b) Requerir que se le comuniquen los datos que se refieran a ella. c) Ser informada de los motivos por los que se le deniegue una petición de conformidad con los derechos anteriores y poder recurrir contra la denegación. d) Impugnar datos que se refieran a ella misma y si la impugnación es correcta requerir que los datos de que se trate sean cancelados, rectificados, completados o modificados.

3. El Convenio del Consejo de Europa

El 28 de enero de 1981 el Consejo de Europa adopta el «Convenio para la protección de las personas con relación al tratamiento automatizado de datos de carácter personal». Es el primer convenio y, por tanto, instrumento internacional jurídicamente obligatorio que regula específicamente esta materia y el único hasta el momento.
En cuanto a la calidad de los datos se dispone que:
a) Han de ser obtenidos y elaborados leal y lícitamente.
b) Han de ser registrados para fines determinados y legítimos y no utilizados de manera incompatible con tales fines.
c) Han de ser adecuados, pertinentes y no excesivos con respecto a los fines.
d) Han de ser exactos.
e) Han de ser conservados en forma que permitan la identificación de los interesados durante un plazo que no exceda del necesario de acuerdo con sus fines.
En relación con las clases especiales de datos, aquellos denominados «sensibles», como el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, los relativos a la salud o a la vida sexual, no podrán ser elaborados automáticamente a no ser que el derecho interno establezca las garantías oportunas. Lo mismo se observará respecto a los datos de carácter personal referentes a conductas criminales.
Bajo la rúbrica de garantías complementarias para el interesado, el Convenio recoge, verdaderamente, derechos básicos de las personas para la protección efectiva de sus datos personales. Para su ejercicio toda persona deberá: a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus fines principales, así como la identidad y residencia habitual o el establecimiento principal del responsable del fichero. b) Obtener, en intervalos razonables, la confirmación de que en ese fichero hay datos personales que le afectan. c) Obtener, en su caso, la rectificación de tales datos o su cancelación. d) Interponer recurso si no es estimada una petición de confirmación o, en su caso, de comunicación, rectificación o cancelación.
Las excepciones y restricciones a estos principios sólo serán posibles en casos y situaciones concretos para la defensa de la democracia, exigiéndose en determinados casos la previsión

Fundación Telefónica
Telefónica

legal.

4. El Acuerdo de Schengen

El «Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 relativo a la supresión gradual de controles en las fronteras comunes», de 19 de junio de 1990, lleva a cabo, también, en su ámbito concreto, una regulación de protección de datos personales. El grado de protección en el marco del Sistema de Información Schengen es, sin embargo, menor que el del Convenio del Consejo de Europa al tener lugar en el específico campo excepcional de la cooperación policial.

Aunque se reconoce el derecho de toda persona para acceder a los datos que se refieran a ella, que estén integrados en el Sistema de Información, su ejercicio estará sometido al derecho del Estado parte ante el que se alegue.

Se establece el derecho de toda persona a que se rectifiquen los datos relativos a ella con errores de hecho y a que se supriman los que tengan errores de derecho.

Se reconoce, también, el ejercicio de acciones ante los tribunales o autoridades competentes a efectos de rectificación, supresión, información o indemnización.

Fuera del Sistema de Información Schengen, el Convenio se ocupa, asimismo, de manera más general, del régimen de la transmisión de datos personales.

5. La Propuesta de Directiva de la Comunidad Europea

El Consejo de las Comunidades Europeas ha elaborado una propuesta de Directiva, presentada por la Comisión el 27 de julio de 1990 que en su actual redacción, de 15 de octubre de 1992, se denomina «Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos» y modifica profundamente en sistemática y contenido la redacción originaria (COM (92) 422 fial. SYN 287. DOCE, C 311, de 27-11-1992).

En la definición de dato personal, se considerará identificable toda persona cuya identidad pueda determinarse directa o indirectamente mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social; no tendrán carácter personal los datos estadísticos en los que los interesados dejen de ser razonablemente identificables.

En cuanto a la calidad de los datos rigen los principios de tratamiento que de un modo u otro son de reconocimiento general y se recogen en todos los instrumentos considerados.

Los datos «sensibles» constituyen, como en el Convenio del Consejo de Europa, una categoría especial cuyo tratamiento queda, en principio, prohibido y en caso de poderse realizar, se han de cumplir condiciones particulares. Las excepciones a la prohibición general de tratamiento de estos datos pueden establecerse por los Estados miembros, por motivos de interés público, mediante una disposición legal o una decisión de la autoridad de control.

Se concede, también, a los Estados miembros la facultad para determinar las condiciones en las que podrá utilizarse un número nacional de identificación o cualquier otro medio de identificación de carácter general.

Bajo la denominación de información al interesado, la Propuesta de Directiva regula los distintos ámbitos en los que tal información ha de tener lugar.

El derecho del interesado de acceso a los datos, se reconoce como derecho a obtener la confirmación de la existencia o inexistencia de datos personales que le afecten, y como derecho a que se proceda a la rectificación, supresión o bloqueo, cuando su tratamiento no se ajusta a la Directiva. El ejercicio del derecho de acceso puede quedar, sin embargo, exceptuado en una serie de aspectos básicos.

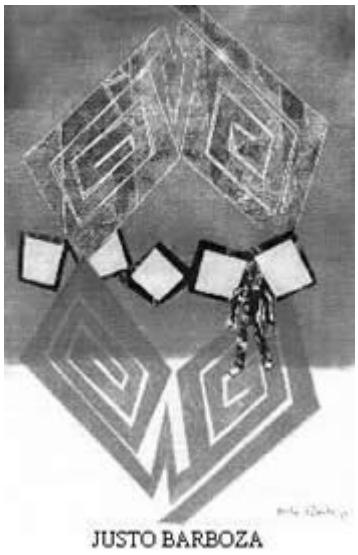
Los derechos del interesado se completan con el derecho de oponerse, en cualquier momento

Fundación Telefónica
Telefónica

y por razones legítimas, a que los datos que le afecten sean objeto de tratamiento; en tal caso el responsable del tratamiento deberá suspender esta actividad.
Por otra parte se reconoce el derecho de las personas de no verse sometidas a una decisión administrativa o privada que les resulte perjudicial, basada únicamente en un tratamiento automatizado que dé el perfil de su personalidad.
En cuanto a los recursos judiciales, la Propuesta de Directiva establece la obligación de los Estados miembros de poner a disposición de toda persona un recurso judicial en caso de violación de los derechos garantizados por la misma.

3. LA REGULACIÓN ESPAÑOLA SOBRE LA PROTECCIÓN DE DATOS PERSONALES

El derecho específico español, en cumplimiento del mandato constitucional del art. 18.4, es el que se recoge en la Ley Orgánica 5/1992, de 29 de octubre, de «Regulación del tratamiento automatizado de datos de carácter personal» (LORTAD) (BOE de 31-10-1992).
1. El ámbito de aplicación
En cuanto al ámbito de aplicación, la Ley se extiende tanto a los ficheros de titularidad pública, como de titularidad privada, así como al uso no automatizado de los datos registrados en soporte físico susceptible de tratamiento automatizado e incluso, en virtud de la Disposición Final Segunda, cabe su extensión, con las condiciones que se establezcan, a los ficheros convencionales. Sin embargo, se establece tal número de excepciones y de regímenes específicos que dejan a la Ley prácticamente vacía en su contenido, teniendo en cuenta, además, que ya existen una serie de excepciones a la aplicación de disposiciones concretas.


JUSTO BARBOZA

Por esta vía de excepción, la Ley no será de aplicación, aparte de a los ficheros de personas físicas con fines personales, a los ficheros automatizados de titularidad pública que tengan por finalidad dar publicidad a los datos de carácter general; a los de información tecnológica o comercial que reproduzcan datos ya publicados en publicaciones oficiales; a los ficheros de informática jurídica accesibles al público, cuando se limiten a reproducir disposiciones o resoluciones judiciales publicadas en publicaciones oficiales; a los ficheros mantenidos por partidos políticos, sindicatos e iglesias, confesiones o comunidades religiosas, cuando los datos

Fundación Telefónica
Telefónica

se refieran a sus asociados o miembros y ex miembros, aunque en este caso la cesión de los datos quedará sometida a la Ley.
Una segunda exclusión incluye a los ficheros que se rigen por sus disposiciones específicas, entre los que se encuentran los regulados por la legislación de régimen electoral; los sometidos a las normas sobre materias clasificadas; los derivados del Registro Civil y del Registro Central de Penados y Rebeldes; los que sirvan a fines estadísticos al amparo de la Ley de la función estadística pública, salvo las competencias que se atribuyen a la Agencia de Protección de Datos; los ficheros cuyo objeto sean los datos de los informes personales bajo la regulación de la Ley del régimen del personal militar profesional.
En tercer lugar, la Disposición Adicional Primera, excluye la aplicación de las disposiciones relativas a la Agencia de Protección de Datos y a la infracciones y sanciones, a los ficheros de los que sean titulares las Cortes Generales, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo General del Poder Judicial y el Tribunal Constitucional.

2. La obtención de los datos

En cuanto a la colecta o recogida de los datos personales y su conservación, la protección de la persona no queda debidamente garantizada al no disponerse más que los datos serán cancelados, en lugar de borrados o destruidos, cuando ya no sean necesarios o pertinentes a su finalidad, a pesar de que, de conformidad con el Convenio del Consejo de Europa y de la Propuesta de Directiva, cuando haya razón para ser conservados se establece la imposibilidad de poderlos identificar. Tan sólo se contempla la destrucción en tal supuesto respecto a ficheros de titularidad privada que presten servicios de tratamiento de datos por cuenta de terceros y, aún así, con diversas excepciones.
La información que se ha de dar a los afectados en la recogida de los datos deviene en obligación enervada, toda vez que no se impone su exigencia si el carácter de la recogida se deduce claramente de la naturaleza de los datos o de las circunstancias en que se recojan. La posibilidad de excepciones a la obligación de informar es todavía mayor respecto a los ficheros de titularidad pública, de tal modo que prácticamente podrá conducir a una exclusión general de la obligación de informar en la recogida de datos.
La exigencia fundamental del consentimiento del afectado para el tratamiento automatizado de datos de carácter personal, que sólo podrá ser revocado con causa justificada y sin efectos retroactivos -salvo en los casos en que la Ley disponga otra cosa-, puede ser fácilmente obviada en la práctica dada la amplitud de las eximentes que se permiten.

3. La cesión de datos

La prohibición de la cesión de datos personales sin el consentimiento del afectado queda seriamente devaluada al excluirse, además de los casos de previsión legal o ser datos de acceso público, aquellos en los que el establecimiento del fichero automático responda a la libre y legítima aceptación de una relación jurídica; las cesiones de datos que hayan de efectuarse al Defensor del Pueblo, al Ministerio Fiscal y a los jueces y tribunales en el ejercicio de sus funciones; las cesiones de unas administraciones públicas a otras cuando hubiesen sido previstas por las disposiciones de la creación del fichero o por disposición posterior de igual o superior rango. Para otros casos, como los datos relativos a la salud, se establecen condiciones particulares.

4. El derecho de acceso

Entre los derechos de las personas en relación con el derecho de acceso para conocer los datos personales que de ellas existan en un fichero, sólo se prevé que cuando resulten inexactos o incompletos sean rectificados y cancelados «en su caso», con cuya apostilla la tímida obligación queda aún más reducida, aparte de las excepciones que se establecen.

Fundación Telefónica
Telefónica

Las excepciones, en este ámbito, llevan a la prohibición de cancelar cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos, con lo que, en el primer caso se llega incluso a sustituir la propia voluntad del interesado; en los otros dos casos debería encomendarse la determinación a una instancia independiente que podía ser la Agencia de Protección de datos a la que ya se requiere por la Ley para situaciones semejantes. También se establecen excepciones al derecho de acceso -permitidas por las normas internacionales- en relación con las fuerzas y cuerpos de seguridad y para la protección de los derechos y libertades de los terceros; no parece, en cambio, suficientemente justificada la excepción del derecho de acceso en relación con los ficheros de la Hacienda Pública.
El procedimiento para ejercer el derecho de acceso debería para mayores garantías, regularse en la propia Ley, al menos en sus características básicas, y no dejarse totalmente al desarrollo reglamentario. La posibilidad de exigir la responsabilidad a través de recursos necesita ser concretada respecto a los ficheros de titularidad privada ya que únicamente se dispone que la acción se ejercerá ante los órganos de la jurisdicción ordinaria, pero ¿de qué orden? ¿a través de qué clase de juicio? ¿cómo se determina la competencia?

4. CONCLUSIONES

En lo que respecta a la conformidad de nuestra Ley al derecho internacional y comunitario en particular, en una consideración general la LORTAD contiene disposiciones no del todo ajustadas a la regulación internacional o que no desarrollan ésta debidamente y otras disposiciones no conducen al resultado pretendido. Por ello, presenta lagunas y en buen número de casos, las garantías para la protección de la persona respecto a sus datos personales se establecen en los mínimos permitidos.
Con relación a los aspectos básicos, la Ley es correcta en la fijación general o de principio de los mismos, pero las disposiciones se quedan vacías de contenido y se hacen, por tanto, inaplicables por vía de excepciones y exclusiones realmente exorbitantes.
Por otra parte, al haberse seguido la originaria Propuesta de Directiva en el Proyecto de Ley, sin tener en cuenta, a la hora de aprobar ésta, la Propuesta actual de Directiva, sustancialmente diferente a la anterior y más conforme a un desarrollo del Convenio Europeo, la Ley nace con un alto riesgo de inadaptación a la futura Directiva, particularmente en la diversidad de regulación de los ficheros de titularidad pública y de titularidad privada que hace nuestra Ley.
Resulta así que esta Ley cubre formalmente una obligación, impuesta por el Convenio Europeo y por el Convenio de Schengen, pero con un escaso compromiso de fondo. Sin embargo, incluso esta apariencia bien puede resultar fallida si la futura Directiva comunitaria, cuya propuesta actual tendrá, a su vez, que ajustarse más al Convenio del Consejo de Europa, invalida la Ley española, máxime si se mantienen las funciones del Grupo de protección de datos personales que se establecen en la actual Propuesta.

Fundación Telefónica
Telefónica