LA AGENCIA DE PROTECCION DE DATOS. FUNCIONES Y POTESTADES SANCIONADORAS

SANTIAGO CABALLERO MENDAÑA
Comandante de la Guardia Civil

LA reciente Carta de Derechos Fundamentales de la Unión Europea acuña en su articulado nuevos derechos fundamentales, además del derecho a la protección de datos de carácter personal, y, entre otros, la prohibición de clonación de seres humanos, la prohibición de prácticas genéticas, particularmente las que tengan por objeto la selección de las personas, etc.

A pesar de que, por el momento, a la Carta no puede atribuírsele más que un valor meramente proclamatorio, creemos que su contenido tendrá un efecto vinculante para las legislaciones de los Estados miembros, en una primera fase, porque se hace difícil imaginar que alguno de estos Estados dicte normativas en contradicción con los derechos declarados, y en una fase posterior, porque su influencia en la conciencia social y en la jurisprudencia acabará forzando la inclusión explícita de los nuevos derechos en las legislaciones.

Este espíritu late en el preámbulo de la Carta cuando declara:

> *"... A este fin, es necesario, expresándolos más visibles en una Carta, reforzar la protección de los derechos fundamentales a la luz de la evolución de la sociedad, del progreso social y de los desarrollos científicos y tecnológicos.*
>
> *La presente Carta reafirma, dentro del respeto de las competencias y funciones de la Comunidad y de la Unión, así como del principio de subsidiariedad, los derechos que resultan en particular de las tradiciones constitucionales y de las obligaciones comunes a los Estados miembros, del Tratado de la Unión europea y tratados comunitarios, de la*

Convención europea de salvaguardia de los derechos del hombre y de las libertades fundamentales, de las Cartas sociales adoptadas por la Comunidad y por el Consejo de Europa, así como de la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas y del Tribunal Europeo de Derechos Humanos.

La posesión de estos derechos conlleva responsabilidades y deberes tanto con respecto del prójimo, como respecto de la comunidad humana y de las generaciones futuras."

Para nuestro objeto de estudio es de especial relevancia significar que, en su Capítulo II "Libertades", la Carta separa clara y definitivamente el respeto de la vida privada y familiar, artículo 7, (1) de la protección de datos de carácter personal, artículo 8, consolidando a éste como un derecho fundamental de libertad de carácter autónomo, del que además precisa su contenido (2):

8.1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen.

8.2. Estos datos deben ser tratados lealmente, para fines determinados y sobre la base del consentimiento de la persona concernida o en virtud de algún fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y obtener su rectificación.

8.3. El respeto de estas reglas será sometido al control de una autoridad independiente.

Las recientes Sentencias del Tribunal Constitucional 290 y 292/2000 acogen el reconocimiento explícito en un nuevo derecho fundamental de reciente configuración: el derecho fundamental a la protección de datos, abandonando las tesis seguidas por la línea jurisprudencial iniciada con la sentencia 254/1993 de 20 de julio, y consolidan el papel fundamental que juega en nuestro ordenamiento la Agencia de Protección de Datos como agente protector de este derecho en todo el territorio nacional.

Ello es así porque, desde que comenzaron a percibirse las amenazas de nuevo tipo que el fenómeno informático introduce con respecto al derecho a la intimidad, para la opinión pública y el pensamiento filosófico, jurídico y político de nuestro tiempo constituye un problema nodal el establecimiento de unas garantías que tutelen a los ciudadanos frente a la eventual erosión y asalto tecnológico de sus derechos y libertades (3), teniendo en cuenta que el mundo de la cibernética ha evidenciado un potencial lesivo para la intimidad, cuya intensidad y eficacia resultaban inimaginables en contraste con las formas históricas de menoscabo de aquel derecho (4).

Un sistema normativo –precisó la STC 143/1994, fundamento jurídico 7º– que, autorizando la recogida de datos incluso con fines legítimos y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta.

TRUYOLS Y VILLANUEVA (5), considerando el daño irreparable que puede sufrir el individuo por la utilización y/o publicidad indebida, dadas a informaciones sobre su intimidad, entienden que, entre las garantías requeridas para una protección eficaz de la intimidad que debe incluir la normativa legal, es necesario incluir como principio que la protección se ejerza preferentemente de un modo preventivo y no sólo o principalmente represivo.

Como destaca LUCAS MURILLO DE LA CUEVA, para el examen de las funciones y potestades no sancionadoras de la Agencia de Protección de Datos, objeto de este trabajo, fijaremos la perspectiva de estudio tomando como referencia fundamental que la Agencia nace y existe para hacer efectivo el derecho a la intimidad. Es decir, se trata de una organización cuya razón de ser es la de ofrecer una primera línea de defensa especializada de este derecho fundamental, sin perjuicio de las demás que a este tipo de derechos reconoce el ordenamiento jurídico (6).

Estos aspectos han sido puestos de manifiesto claramente por la Sentencia del Tribunal Constitucional 290/2000 de 30 de noviembre, a la que nos seguiremos refiriendo a lo largo del trabajo.

Partiendo de todo ello, trataremos de ofrecer el adecuado perfil de la posición que este órgano ocupa y de la misión que está llamado a desempeñar, justificando en primer lugar la necesidad y la naturaleza de un elemento institucional de garantías.

NECESIDAD DE UNA AUTORIDAD DE CONTROL

Justificación de la necesidad y naturaleza de la autoridad de control

SPIROS SIMITIS, primer comisario encargado de la protección de datos en la República Federal de Alemania, en el "Informe de síntesis" de las sesiones del seminario de París, organizado por la OCDE, del 24 al 26 de junio de 1974, *Questions d'ordre politique soulevés par la protection des donnés et des libertés individuelles*, señaló que sin organismos públicos independientes que supervisaran el cumplimiento de las prescripciones legales no era factible un control del funcionamiento de los bancos de datos ni una valoración de los resultados y los avances técnicos con relación al grado de respeto de las leyes (7).

Todas las leyes de protección de datos que se han ido promulgando desde 1970 han creado una autoridad especializada para su aplicación. Unicamente la *Privacy Act* norteamericana se abstuvo de crear una tal autoridad, encomendando a los tribunales ordinarios la solución de los litigios que surgieran en la aplicación de la ley. Sin embargo, esta solución no es conciliable con el carácter preventivo del sistema protector de datos que estas leyes configuran (8):

- En primer lugar porque la intervención de los órganos judiciales requiere que se haya *producido el litigio y, por tanto, el daño o perjuicio imputable a la recogida y el uso indebido de los datos.*
- Por otra parte, la aplicación del sistema protector, con el consiguiente registro de ficheros o equivalente, que haga posible el ejercicio del derecho de información, requiere una acción administrativa de gestión y una ordenación por vía reglamentaria.

Ahora bien, si la solución judicial no es idónea, la necesidad de una acción conformadora hace que la opción del Comisario parlamentario no sea tampoco suficiente por sí sola.

Ante la duda sobre la conveniencia de encomendar las funciones de garantía al Defensor del Pueblo, debe significarse que la determinación constitucional prevista en el artículo 54 en cuanto a su ámbito de actuación –la Administración– es un importante obstáculo para escoger este camino, habida cuenta que si se entiende que no puede extenderse el campo de actuación del Defensor más allá de las Administraciones Públicas para abarcar, también, las relaciones jurídico-privadas, sin desnaturalizar esta institución, entonces será necesario utilizar otra vía, pues es imprescindible para el respeto a la autodeterminación informativa el control de la actividad informática privada en el campo de los datos personales (9).

Por tanto, y por la importancia que revisten las normas de procedimiento, como signo emblemático de la peculiaridad de la tutela jurídica de los derechos de la tercera generación, se impone una solución institucional especializada de protección, que tienda a completar la función de garantía de los Tribunales.

Esto no implica que la autoridad especializada excluya toda actuación de los órganos jurisdiccionales ni tampoco del Parlamento. Todas las legislaciones prevén una revisión judicial de los actos de esta autoridad, así como algún tipo de control parlamentario que se encauza por la vía de una información anual o periódica en forma de memoria oficial.

Esta solución garantista mediante un elemento institucional, está presente en las regulaciones legales adoptadas antes de la entrada en vigor de nuestra Constitución por varios Estados europeos, con la finalidad de *proteger los datos personales frente a los peligros de la informática (Ley sueca de 11 de* mayo de 1973, Ley de la República Federal de Alemania, de 22 de enero de 1977, Ley francesa de 6 de enero de 1978, Ley noruega de 8 de junio de 1978)

Dichas regulaciones, pese a las diversas denominaciones y dependencias orgánicas que establecen, tienen en común haber creado instituciones especializadas de De-

recho público, a las que se atribuyen diversas funciones de control sobre los ficheros de datos personales susceptibles de tratamiento automatizado, tanto de titularidad pública como privada.

Aceptada esta solución, Pérez Luño (10) hace notar el protagonismo adquirido por las variantes del sistema general del Ombudsman, específicamente dirigidos a la protección de los ciudadanos respecto al tratamiento informatizado de datos personales, destacando que, entre las ventajas que ofrece el sistema general del Ombudsman para la protección efectiva de los derechos fundamentales, pueden citarse las referidas a las funciones siguientes:

- *Función dinamizadora, adaptadora y de reciclaje de los derechos fundamentales,* realizada básicamente a través de los informes periódicos presentados ante los Parlamentos, de los que son comisionados.
- *Función orientadora de los ciudadanos,* agilizando y clarificando los procedimientos de tutela de las libertades.
- *Función preventiva de las agresiones a los derechos humanos,* evitando agresiones y daños de difícil o imposible reparación en el ejercicio de tales derechos; ya que al ejercicio de las libertades es de cabal aplicación el célebre adagio latino: *melius est preveaire quam reprimere.*

Sin embargo, hasta la primera propuesta de Directiva comunitaria sobre protección de datos (SYN 287, 1990) no existe lo que podría denominarse una "teoría general" de la Autoridad especializada de protección de datos. El término de "Autoridad de control" no aparece hasta entonces como expresivo de un concepto genérico, pues, si bien existió siempre un acuerdo acerca de la necesidad de una tal autoridad y de la insuficiencia de la autoridad judicial, sin embargo, cada autoridad en concreto de las creadas por la legislación comparada hasta ese momento se basa en una concepción distinta.

Seguiremos el articulado de la propuesta, toda vez que, en esta primera parte, conectaremos su contenido con la Ley Orgánica 5/1992, de 29 de octubre (LORTAD), en lugar de referirnos a la Directiva 95/46, de publicación posterior.

Modelo de la autoridad de control

La propuesta de Directiva –tanto la versión primitiva de 1990, como la de 1992– define un modelo a tal efecto en el artículo 30, completado por otros preceptos dispersos. Este modelo es fruto, a la vez, de un proceso de unificación y de una "extrapolación". La Comisión quiso incluir en la pauta estructural y competencial que define el precepto, características que ya estaban presentes en todas las autoridades de control preexistentes. Pero asimismo añadió algunas que, o bien estaban sólo apuntadas o definidas de manera imperfecta en la mayoría de autoridades o sólo se daban en algunas de ellas.

El resultado es que ninguna de las autoridades existentes se ajusta totalmente al modelo de la propuesta de Directiva: todas carecen de alguna o algunas de tales características. Por otra parte, éstas no están claramente definidas y permiten cierta variedad de opciones concretas (11).

Características de la autoridad de control.

La primera de las características que definen el modelo de la propuesta de Directiva es la de *independencia* (art. 30-1).

No se especifica en el precepto ni en los considerandos lo que deba entenderse por "autoridad independiente", por lo que el concepto puede ser entendido en varios planos: designación del titular, exterioridad a la estructura de la Administración del Estado, determinación del contenido de los actos, dotación de medios personales, materiales y financieros necesarios para el funcionamiento, revisión de los actos.

Conforme a ello, podría entenderse que el órgano es independiente si el titular es designado por el Parlamento o el Jefe del Estado, no está encuadrado en la estructura de la Administración, los titulares no están sujetos a instrucciones en cuanto al contenido de los actos, el ente tiene medios propios y sus actos sólo son susceptibles de control de legalidad en sede jurisdiccional.

Sin embargo el elemento esencial que permite calificar a un ente público como independiente es la no sujeción de sus actos a instrucciones de ningún otro órgano. El hecho de que la autoridad de control sea designada por el Parlamento, por un Gobierno, o por un Ministro o por el Jefe del Estado, resulta irrelevante. La designación parlamentaria, en sí misma, puede acarrear un riesgo de politización, en la medida en que la elección del titular pueda estar mediatizada por la correlación de las fuerzas políticas (12).

La independencia se refleja asimismo en la ausencia de un control jerárquico, en la "exterioridad" de la autoridad de control con respecto a la estructura de la Administración del Estado. Esta nota va íntimamente ligada a la no sujeción de instrucciones. Sólo cabe un control de legalidad por parte de los órganos de la jurisdicción.

En cuanto a su *concepción*, la propuesta no limita a una sola la autoridad de control. El artículo 30-1, permite que cada Estado designe varias autoridades de control, lo que autoriza para entender:

- Que la autoridad de control esté compuesta por varias, v. gr. Titular y Consejo.
- Que existan varias autoridades en función de la implantación territorial.
- Que exista una pluralidad de autoridades por razón de la materia.

Por lo que respecta a las *funciones*, la propuesta de Directiva comprende unas funciones determinadas:

- En primer lugar una función genérica de "ejercer el control de la protección de datos personales", acotada por el propio precepto a la vigilancia de la aplicación de las disposiciones nacionales en aplicación de la Directiva, habida cuenta que el control de la protección de los datos personales objeto de tratamientos que no entren en el ámbito de aplicación del Derecho comunitario no será competencia de la autoridad de control. Para posibilitar el ejercicio de esta función genérica, se contempla la atribución de potestades administrativas:
  - *Potestad de investigación:* Acceso a los datos que sean objeto de tratamiento y de recabar toda información necesaria para el ejercicio de la función de control
  - *Potestad de intervención:* Ordenar el bloqueo o la supresión de datos, prohibición provisional o definitiva de tratamientos, destrucción de soportes de datos o formulación de advertencias o apercibimientos a los responsables de los tratamientos.

A estas dos potestades se añade la potestad de denuncia a la autoridad judicial cuando haya comprobado la existencia de infracciones a las disposiciones nacionales adoptadas en aplicación de la Directiva. En las legislaciones que atribuyen potestad sancionadora a su autoridad de control, ésta deberá entenderse como una función complementaria.

- Otras funciones contempladas en el artículo 30:
  - Sustanciar reclamaciones y denuncias.
  - Cooperar con las demás autoridades de control.
  - Redactar una memoria anual que deberá ser publicada.
- Funciones que habilitan a la autoridad de control para la derogación singular de algunos de los preceptos básicos de la Directiva:
  - Respecto de los datos sensibles, cuyo tratamiento se prohíbe como norma general.
  - En cuanto a la obligación de informar al afectado en caso de comunicación de sus datos a un tercero, cuando el consentimiento para el tratamiento no sea preceptivo, o cuando sea imposible informarle o cuando ello implique esfuerzos desproporcionados o se oponga a los intereses legítimos del responsable del tratamiento o de un tercero.
  - Exceptuar el derecho de acceso un determinado tratamiento, a petición del afectado, procediendo a las averiguaciones necesarias.

- Exceptuar de la obligación de notificar o prever una notificación simplificada.

– Resto de funciones, no contempladas en el artículo 30:

- Función de autorización previa para los tratamientos que impliquen riesgos especiales para los derechos y libertades de las personas.
- Comprobar la procedencia y representatividad de los códigos de conducta.
- Función certificante, en cuanto atribuye a la autoridad de control la llevanza del registro de los tratamientos.

Sin embargo, la propuesta de Directiva no atribuye a la autoridad de control competencia alguna en lo que respecta a la autorización de transferir datos a terceros Estados cuyo nivel de protección no sea el adecuado, cuestión sobre la que profundizaremos en el último apartado, por estimarla de especial trascendencia.

MODELO ESPAÑOL. LA AGENCIA DE PROTECCION DE DATOS COMO AUTORIDAD DE CONTROL INDEPENDIENTE

El artículo 34.1 de la LORTAD, hoy recogido por el artículo 35.1 de la Ley Orgánica de Protección de Datos, 15/1999 de 13 de diciembre (LOPD), creó la Agencia de Protección de Datos y el Real Decreto 428/1993, de 26 de marzo, la dotó de un estatuto, cumpliendo lo dispuesto en el artículo 34.2 y disposición final primera de la LORTAD, procedimiento que ha suscitado críticas (13), pero en el que no nos detendremos.

Siguiendo el criterio del Consejo de Estado, (Dictamen 97/93), se optó por un texto limitado a la estructura orgánica y funcional de la Agencia y a su régimen jurídico, económico, presupuestario y de personal, postergando el resto de desarrollo reglamentario hasta la efectiva constitución de la Agencia y nombramiento de su Director, habida cuenta que, conforme al artículo 36 h) de la LORTAD –hoy 37 h) de la LOPD–, la Agencia debe informar preceptivamente los proyectos de disposiciones generales que desarrollen la Ley.

El legislador ha optado por un órgano especializado de control de su aplicación definiendo una solución original, adecuada al contexto jurídico-administrativo español (14), mediante un modelo ecléctico entre las opciones individual o colegiada, pero inspirado en la Ley federal alemana de 27 de enero de 1977, modificada el 20 de diciembre de 1990, situando a un Director/Comisario Federal como órgano de dirección de la Agencia, prescindiendo de otro tipo de órganos pluripersonales, a manera de Comisión (15).

La configuración de la Agencia, con el Consejo Consultivo como "colegio electoral" del Director, es fruto de la transacción, toda vez que en el proyecto del Gobierno sólo figuraba el Consejo como órgano de asesoramiento del Director. El resultado final se plasma en los artículos 34 a 41 de la LORTAD –y sus equivalentes 35 a 42 de la LOPD– que establecen a la Agencia como un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad jurídica, pública y privada, encuadrado en el género definido por el artículo 6.5 de la Ley General presupuestaria (Texto Refundido aprobado por Real Decreto Ley 1091/1998)

Ajuste de la Agencia al modelo

La opción escogida por el legislador español, se ajusta al modelo definido en el artículo 30 de la propuesta de Directiva, en los términos antes vistos. La característica de independencia se recoge en el artículo 35.1 de la LOPD, artículo 16.2 del Estatuto y se complementa con las disposiciones recogidas en los artículos 15, 17, 19 y 20 del Estatuto.

Además, ni la Agencia ni el Director están sujetos a modalidad alguna de tutela administrativa. Sólo existe un control de legalidad de los actos del Director, por el cauce del recurso contencioso-administrativo previsto en los artículos 35.2 y 18.4 de la LOPD y 24 del Estatuto.

No obstante, la ausencia de tutela administrativa es compatible con la existencia de unos cauces de relación con los poderes del Estado, previéndose por el Estatuto los siguientes:

a) Entre la Agencia y el Gobierno, por conducto del Ministro de Justicia, artículos 1.2 y 19.2.

b) Con las Cortes Generales, en la forma de traslado de la Memoria Anual de la Agencia a las Cortes por el Ministro de Justicia, artículo 8.2.

c) Con el Tribunal de Cuentas, a través de la Intervención General de la Administración del Estado, artículo 33.1.

Por otra parte, la "exterioridad" de la Agencia respecto a la estructura de la Administración, como un aspecto mas de la característica de la independencia, se refleja en el artículo 33.3 del Estatuto, al regular el control financiero en forma de control permanente, incompatible con la fiscalización previa, y, aún cuando sometida al control del Tribunal de Cuentas, éste no constituye una tutela, sino un control de otra naturaleza.

A los mismos resultados llega LOPEZ RAMON a través del análisis de los elementos normativo, personal, funcional, financiero y relacional de la Agencia (16).

Sin embargo, a nuestro juicio, la nota que, en teoría y en la práctica, mejor garantiza la independencia, es la regulación contenida en el artículo 35.5 de la LOPD, al establecer que la Agencia elaborará y aprobará con carácter anual el correspondiente anteproyecto de Presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado. Con ello, y con la preeminencia de la figura del Director que trataremos a continuación, creemos que se evidencia la intención de crear un órgano que funcione eficazmente.

Respecto de la argumentación expuesta el punto 1 anterior, para justificar la necesidad de un elemento institucional de garantías, ya desde la regulación de la LORTAD se desprende un rasgo significativo de la Agencia de Protección de Datos: *el carácter básicamente preventivo de sus funciones en orden a la protección de datos personales.* Un rasgo caracterizador que es común a las instituciones especializadas existentes en los países de nuestro entorno y al que hace referencia la Exposición de Motivos, al afirmar que esta disposición está guiada por la idea de implantar mecanismos cautelares que prevengan las violaciones de los derechos fundamentales.

En efecto, al dar cumplimiento al mandato contenido en el artículo 18.4 CE, el legislador, sin excluir en modo alguno el recurso último a los órganos jurisdiccionales para la tutela de los derechos individuales, como se determinaba en los apartados 2 a 5 del artículo 17 LORTAD –actualmente recogidos en los puntos 2 a 4 del artículo 18 de la LOPD– no ha querido sin embargo que la protección de datos personales frente al uso de la informática se lleve a cabo exclusivamente en la vía judicial, esto es, cuando ya se ha producido una lesión del derecho fundamental.

Por el contrario, ha querido que dicha protección se lleve a cabo mediante el ejercicio por la Agencia de Protección de Datos, con carácter básicamente preventivo, de las funciones de control de los ficheros tanto de titularidad pública como privada que la LOPD le atribuye y, en su caso, a través de las reclamaciones de los afectados ante la Agencia de Protección de Datos (art. 18.1 de la LOPD), las que provocarán la posterior actuación de este órgano.

Por ello cabe estimar que existe una correspondencia entre las funciones y potestades que la LOPD ha atribuido a la Agencia de Protección de Datos y el carácter preventivo de sus actuaciones, y es este carácter tuitivo o preventivo el que, en última instancia, justifica la atribución de tales funciones y potestades a la Agencia de Protección de Datos para asegurar, mediante su ejercicio, que serán respetados tanto los límites al uso de la informática como la salvaguardia del derecho fundamental a la protección de datos personales en relación con todos los ficheros, ya sea de titularidad pública o privada (17).

Respecto de la LORTAD, la LOPD mantiene la configuración de la Agencia, introduciendo variaciones mínimamente relevantes, de las que resaltamos como significativas para el objeto de estudio:

- El aumento de funciones del Director, para incluir el derecho de oposición.
- Igualmente, la facultad de éste para requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas

necesarias para la adecuación de los tratamientos de datos a las disposiciones de la Ley.
- La composición del Consejo consultivo no se altera salvo que en lugar de haber un representante del conjunto de las Comunidades Autónomas, habrá uno de cada una de las que haya creado una Agencia de Protección de Datos en su ámbito territorial (18).

El Director de la Agencia

El riesgo de ineficacia que pudiera derivarse de la complejidad para adoptar decisiones, ante la composición multitudinaria de un órgano, de los que existen ejemplos entre los actualmente existentes en la Administración, parece haberse soslayado por la preeminencia concedida a la figura del Director de la Agencia, a tenor de las funciones que se le atribuyen en los artículos 35 y 36 de la LORTAD, mantenidas por los artículos 36 y 37 de la LOPD.

El Estatuto, en sus artículos 2.3, 2.4 y 12, ha resuelto las ambigüedades que el texto de la Ley ofrece en cuanto a una posible distribución de funciones entre el Director y la Agencia, en la medida en que la Ley atribuye las funciones unas veces al Director y otras a la Agencia, al disponer que "la Agencia ejercerá sus funciones por medio del Director, a cuyo efecto los actos del Director se consideran actos de la Agencia"

Para mayor concreción, las funciones de dirección, órgano de decisión institucional, se rematan en el artículo 12.2, a cuyo tenor corresponde al Director "dictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia". A estos efectos, el precepto contiene una enumeración ad exemplum de las funciones que, por ello, son actos del Director y actos de la Agencia. Puede decirse por tanto que el Director es el eje sobre el que pivota toda la actividad de la Agencia, llegando a afirmarse por algún autor que *la Agencia es el Director* (19).

Además la Ley confiere al Director las funciones de gestión derivadas del artículo 12.1: "dirige la Agencia y ostenta su representación" y especificadas en el artículo 13 (contratación, ordenación de gastos y pagos...). Son estas funciones las que, a diferencia de las del artículo 12 cuyo cauce es la legislación de procedimiento administrativo, no constituyen "funciones públicas de la Agencia", regidas por las disposiciones del Capítulo IV del Estatuto, que en general se remiten a la legislación presupuestaria y respecto de adquisiciones y contratos y régimen patrimonial, al Derecho privado.

Reiterando lo que antes apuntábamos, con tal atribución de funciones y con la independencia presupuestaria, creemos que el propósito ha sido crear un órgano con capacidad funcional efectiva (20).

FUNCIONES DE LA AGENCIA. REFERENCIA A LAS FORMAS DE MATERIALIZACION

Para comenzar este apartado es obligado efectuar una nueva referencia a la Sentencia del Tribunal Constitucional 290/2000, que en su Fundamento Jurídico 15º justifica en la garantía de los derechos fundamentales exigida por la Constitución, así como en la igualdad de todos los españoles en su disfrute, y por tanto declara conforme a la Constitución, el ejercicio por la Agencia de las funciones y potestades a las que nos vamos a referir, también respecto a los ficheros de titularidad privada radicados en las Comunidades Autónomas.

Función genérica

Las funciones de la Agencia se ajustan en general al modelo de la propuesta de Directiva comunitaria de protección de datos. La función genérica se recoge en el artículo 37 a) de la LOPD "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 los datos".

Ahora bien, esta función genérica se manifiesta de dos formas distintas, ya que encomienda a la Agencia de Protección de Datos:

- La vigilancia de la correcta actuación de los operadores del sistema, su adecuación a los principios que se establecen en la Ley.

- La actuación en tutela de los derechos de las personas.

La diferencia que existe entre las dos formas de actuación es enorme, puesto que:

- En el primer caso, la actuación de la Administración será la de policía o control, de oficio y en virtud de un mandato legal, pudiendo establecer pautas de funcionamiento y sanciones en el caso de que la actividad del operador se desarrolle incumpliendo las condiciones que se establecen en la Ley.

  La finalidad del control es el mantenimiento del orden público respecto del tratamiento de los datos, el equilibrio respecto de los intereses confrontados. A través de su ejercicio deben controlarse los tratamientos, la actividad en general, no siendo oportuna la comprobación, dato por dato, para ver si se ha cumplido la norma, sino la tendente a verificar si el tratamiento en sí está diseñado para cumplir la norma. Interesa el bosque y no el árbol (21).

  La responsabilidad que surge en el caso de incumplimiento es carácter absoluto, atiende a que un tratamiento, en su conjunto, pueda no adecuarse a la norma jurídica, en cuyo caso será ilegal por no cumplir las condiciones que se exigen en la Ley.

  Por tanto, para el nacimiento de responsabilidad en estos casos no es necesario que exista una víctima, puesto que la función que se atribuye a la Agencia es de control del orden público que se diseña en la Ley, del buen funcionamiento de los tratamientos y de los operadores, de modo que deberá desarrollarla siempre de oficio, sin necesidad de que nadie inste su ejercicio. El interés que se protege es exclusivamente público, no se trata de amparar la intimidad de un ciudadano concreto, sino de garantizar que el funcionamiento de los operadores es correcto, lo que supone una garantía general de la intimidad protegida, pero no una tutela de ésta.

  Consecuentemente, el sistema de control deberá llevarse a cabo por medio de comprobaciones genéricas, auditorías, en que se observe íntegramente la organización del tratamiento y los sistemas de actuación del operador, para lo cual la Agencia dispone de las potestades administrativas a que se refiere la propuesta de Directiva, antes enunciadas, en correspondencia con el carácter público de sus funciones:

  - *Potestad de intervención:* a que se refiere el artículo 37 f) de la LOPD, con garantía de eficacia mediante la tipificación del artículo 44.4 d) y, como último remedio de la cascada de medidas coercitivas previstas en la Ley, la potestad atribuida por el artículo 49 para inmovilizar los ficheros, pero a los solos efectos de restaurar los derechos de las personas afectadas.
  - *Potestad de investigación:* recogida en el artículo 37 i) y 40 de la LOPD y 28 del Estatuto.
  - *Potestad de denuncia:* mediante una doble vía: en primer lugar en el marco de un expediente sancionador incoado a tenor de lo previsto en el artículo 37 g) de la LOPD, si de las actuaciones del expediente resulta que los hechos son constitutivos de delito. En segundo lugar, la Agencia, en cuanto persona jurídica dotada de plena capacidad pública y privada, puede ejercer acciones civiles y criminales, al amparo de lo previsto en el artículo 38 del Código Civil, y en consecuencia ejercer la acción pública y denunciar los hechos al ministerio Fiscal o al órgano jurisdiccional competente.
  - *Potestad sancionadora:* que la Agencia ha de ejercer en los términos previstos en el Título VII, artículo 37 g) de la LOPD, con la particularidad, cuando se trate de infracciones de una Administración Pública, que tal potestad queda limitada a la facultad de dictar una resolución indicando las medidas que han de adoptarse para corregir el incumplimiento de las previsiones legales en esta materia (art. 46), lo que ha suscitado críticas doctrinales unánimes.

- En el segundo caso, la actuación en tutela de los derechos de las personas, tiene una naturaleza distinta, ya que para que pueda llevarse a cabo es preciso que exista una víctima del incumplimiento de alguna garantía legal, de modo que la persona que se sienta vulnerada en su derecho fundamental a la intimidad puede solicitar el auxilio de la Agencia, para que ésta obligue al responsable de la violación a adecuar el tratamiento de los datos de esta persona a la Ley.

  Por tanto, en este caso la potestad de la Agencia no es de policía o control, sino que se refiere a la protección de la intimidad de un ciudadano concreto que solicita la tutela, debiendo limitarse a atender la instancia del particular ofendido conforme a su petición, y, si no solicita la apertura de expediente sancionador, la Agencia no estará legitimada para abrirlo, puesto que la pretensión del interesado se limita a que se regularice el tratamiento de sus datos.

  En este tipo de actuaciones no es posible la actuación de la Agencia sin la previa denuncia del interesado puesto que lo que se protege no es el funcionamiento correcto de un tratamiento, sino que trata de imponerse una sanción por la violación de la intimidad de un ciudadano. En este caso debe contemplarse el árbol y no el bosque (22).

  Cabe así distinguir dentro de la Ley la existencia de ciertas obligaciones que no tienen por objeto proteger el interés público del correcto funcionamiento del sistema, sino la intimidad de cada particular, como es la vinculación de los datos a la finalidad consentida, la prohibición de cesión sin el consentimiento del interesado, la obligación de atender los derechos de acceso, rectificación, cancelación u oposición, etc.

  En todos estos casos concurre una circunstancia común, la de que el incumplimiento de la ley no es objetivo o absoluto, sino que depende de la actitud del interesado, subjetivamente, que puede entender, o no, que existe una violación de sus derechos, de modo que solo existirá una violación de la intimidad en el caso de que el tratamiento de los datos relativos a un interesado se realice contra su voluntad.

Por tanto, en caso de que el tratamiento esté consentido, no podrá entenderse que exista una violación del derecho protegido, estableciendo el artículo 18 de la LOPD el principio general de tutela, que no implica que la intervención de la Agencia haya de tramitarse mediante un procedimiento sancionador.

Para ello la Agencia goza de una *potestad de resolución de las reclamaciones* de los afectados por incumplimiento de las previsiones de dicha Ley, artículo 37 d) en relación con el artículo 18.1, ambos de la LOPD, y con sujeción al procedimiento establecido por el Real Decreto 1332/1994 (RDLORTAD).

Y, para el caso de que el responsable del tratamiento no haya satisfecho debidamente las pretensiones del ciudadano, el artículo 18.2 regula otro procedimiento que la LOPD denomina *de tutela de los derechos,* que se substanciará por el cauce del artículo 17 del RDLORTAD.

Otras funciones

Además de la función genérica que acabamos de exponer, en sus dos vertientes, y de las potestades administrativas atribuidas para su ejercicio, corresponden asimismo a la Agencia:

- *La función informativa y de publicidad registral,* que el artículo 21 de la propuesta de Directiva atribuye a la autoridad de control, tiene su correspondencia en la función que la Ley española ha instrumentado mediante el Registro General de Protección de Datos del artículo 39 de la LOPD y la obligación del artículo 37 j) de velar por la publicidad de la existencia de los ficheros, a cuyo efecto publicará periódicamente una relación periódica de los mismos. Además se comprende en esta función la información a las personas contemplada en el artículo 37 e) y 4.1 del Estatuto de la Agencia y la publicación y remisión de la memoria prevenida en el artículo 37 k).

- *Función de control y autorización,* prevista en la LOPD o en las disposiciones de desarrollo de aplicación a ésta, artículo 37 b); las que procedan en relación con los movimientos internacionales de datos y las de cooperación internacional en esta materia artículo 37 1) y la del artículo 32.3, en la medida que puede denegarse la inscripción de Códigos tipo en el Registro General.
- *Función integradora y de cooperación al desarrollo normativo,* dictando las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la LOPD [art. 37, apartado c) y m) in fine], cometido trascendente en cuanto fija la interpretación que ha de darse a la Ley, y además informar los proyectos de disposiciones generales a tenor del artículo 37 h) de la LOPD
- *Función de cooperación internacional:* a la que alude el artículo 37 l) de la LOPD

ESPECIAL REFERENCIA A LAS FUNCIONES DEL DIRECTOR EN CUANTO A LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

Efectuamos una especial referencia a las funciones del Director de la Agencia en lo que se refiere a las transferencias internacionales, atendiendo a que, pese a resultar tanto en la Directiva 95/46 como en la LOPD, una de las actividades que se regulan con más cautela, el artículo 33.1 de la LOPD y 12 d) del Estatuto residencian expresamente en el Director la responsabilidad de autorizar tales transferencias cuando el país de destino "no ofrezca un nivel de protección equiparable", pero se hayan "obtenido garantías adecuadas".

El artículo 33.2 de la LOPD pretende contener los criterios a que debe atender la Agencia para evaluar el "carácter adecuado" del nivel de protección, sin embargo no dejan de ser conceptos imprecisos, que exigen que la adecuación deberá ser determinada mediante una valoración de conjunto del sistema de protección.

Por otra parte, la LOPD no ha introducido claridad en la anterior situación, puesto que la disposición adicional primera del RDLORTAD establece que *"se faculta al Ministro de Justicia e Interior para que, previo informe del director de la Agencia de Protección de Datos, apruebe la relación de países que, a efectos de lo dispuesto en el artículo 32 de la Ley Orgánica 5/1992, se entiende que proporcionan un nivel de protección equiparable al de dicha ley"*, de lo que puede deducirse que no existe una competencia exclusiva de ninguna autoridad, ya que esta disposición sólo faculta, pero no atribuye en exclusividad la competencia, ni permite por exclusión del resto entenderla atribuida con este carácter.

En cualquier caso, el sistema que establece la LOPD habrá de interpretarse en el sentido más conforme a la Directiva, y por ello, entender que no puede efectuarse ninguna exportación de datos a países terceros salvo que la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, declare respecto de alguno de estos países que garantiza un nivel de protección adecuado –artículo 34 k) de la LOPD– o se hayan declarado como destinos seguros por el Ministerio de Justicia o se haya obtenido previamente una autorización de la Agencia de Protección de Datos.

Por lo que respecta a la normativa comunitaria, las Decisiones de la Comisión 518 y 519/2000 de 26 de julio (23) establecen un nivel de protección adecuado para Suiza y Hungría, y las Órdenes de 2 de febrero de 1995 y de 31 de julio de 1998, del Ministerio de Justicia, aprueban y amplían, respectivamente, las primeras relaciones de países con protección de datos de carácter personal equiparable a la Ley española, lo que constituye un primer ámbito delimitador.

El segundo de estos ámbitos está configurado por los terceros Estados en el concepto de la Directiva, ya que ésta establece el sistema de protección de datos sobre la base del principio de que los datos de carácter personal constituyen bienes que se integran dentro del comercio, de modo que las libertades de tránsito de bienes, personas y servicios que se establecen como libertades básicas para la consecución de la Unión Europea, se aplican de forma idéntica a cualquier otro bien objeto del comercio que se halle en el ámbito de la UE.

En consecuencia, en el concepto de la

Directiva, sólo existe transferencia internacional de datos cuando el destino es un tercer Estado, un Estado no miembro de la Unión. Por tanto, el sistema de cautelas es aplicable exclusivamente a movimientos de datos hacia, o entre, terceros países, siendo enteramente libre el movimiento de datos de carácter personal entre los Estados parte de la UE (24), sin perjuicio de aplicarse las disposiciones de la LOPD y de la competencia de la Agencia de Protección de Datos para verificar su cumplimiento (25).

Delimitados así estos dos ámbitos territoriales, procede ahora examinar los principios que deben tenerse en cuenta para otorgar la autorización cuando el país de destino es un tercer Estado, al que no se reconoce un nivel de protección equiparable, para lo cual los criterios contenidos en el artículo 33 parecen insuficientes.

El Grupo de Trabajo sobre la protección de datos de carácter personal en lo que respecta al tratamiento de datos personales (WP-DP), creado al amparo del artículo 29 de la Directiva, en su documento de trabajo de 24 de julio de 1998, "Transferencia de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", dedica el Capítulo I a establecer los principios que deben conducir a entender una protección como adecuada.

Así, destaca como evidente que todo análisis significativo de la protección adecuada debe comprender dos elementos básicos: el contenido de las normas aplicables y los medios para asegurar su aplicación eficaz. Tomando como punto de partida la Directiva 95/46, y teniendo en cuenta las disposiciones de otros textos internacionales sobre protección de datos, trata de especificar un "núcleo" de principios de contenido de protección de datos y de requisitos de procedimiento/aplicación cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección.

A pesar de ellos, el grado de riesgo que la transferencia supone para el interesado, se reconoce como un factor importante para determinar los requisitos concretos de un caso determinado.

Principios de evaluación del carácter adecuado del nivel de protección del país de destino

Principios de contenido.

Principios básicos:

- *Principio de limitación de objetivos:* Los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones admitidas serían las contenidas en el artículo 13 de la Directiva.
- *Principio de proporcionalidad y de calidad de los datos:* Los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.
- *Principio de transparencia:* Debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas son las que corresponden al los artículos 11.2 y 13 de la Directiva.
- *Principio de seguridad:* El responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.
- *Derechos de acceso, rectificación y oposición:* El interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho de rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.
- *Restricciones respecto a transferencias*

sucesivas a otros países: Unicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la Directiva.

Principios adicionales de aplicación a tipos específicos de tratamientos:

- *Datos sensibles:* Cuando se trate de categorías de datos sensibles (las incluidas en el artículo 8 de la Directiva), deberán establecerse protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para el tratamiento.
- *Mercadotecnia directa:* En el caso de que el objetivo de la transferencia de datos sea la mercadotecnia directa, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.
- *Decisión individual automatizada:* Cuando el objetivo de la transferencia sea la adopción de una decisión en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

Mecanismos del procedimiento de aplicación.

Se reconoce en el documento que en Europa existe un amplio consenso sobre la necesidad de plasmar los principios de la protección de datos en la legislación. También es amplio el consenso en que un sistema de "supervisión externa" en forma de una autoridad independiente es una característica necesaria de un sistema de cumplimiento de la protección de datos. Sin embargo, en otras partes del mundo no siempre se encuentran estas características.

Con el fin de sentar las base para evaluar el carácter adecuado de la protección ofrecida, es necesario distinguir los objetivos de un sistema normativo de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos de procedimientos judiciales y no judiciales utilizados en terceros países.

Los objetivos de un sistema de protección de datos son básicamente tres:

- *Ofrecer un nivel satisfactorio de cumplimiento de las normas:* Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que los son los sistemas de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos.
- *Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos:* El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia y sin costes excesivos. Para ello es necesario que haya algún mecanismo institucional que permita investigar las denuncias de forma independiente.
- *Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas:* Este es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.

Por el procedimiento de aplicar estos principios a los países que han ratificado el Convenio 108 del Consejo de Europa, a la autorregulación y a las disposiciones contractuales, y tras una evaluación de las excepciones al requisito de protección adecuada, previstas en el artículo 26.1 de la Directiva, aspectos en los que no nos hemos detenido, el Grupo de Trabajo finaliza el documento con tres ejemplos que muestran la utilidad de aplicar estos principios al caso concreto, para determinar si concurren o no garantías adecuadas.

Garantías solicitadas a los responsables de los ficheros (26)

La petición de autorización de transferencias internacionales de datos efectuada al amparo del artículo 33 de la LOPD, exige una serie de garantías que deben ser prestadas por la entidad que realiza la transferencia, como responsable de los ficheros. Así, deberá garantizar el cumplimiento de todas las obligaciones y derechos establecidos en la Ley, y además que se continuará facilitando desde España el ejercicio de los derechos de acceso, rectificación y cancelación de los datos almacenados en terceros países.

El Director de la Agencia viene exigiendo las garantías que se exponen a continuación:

a) Toda la información de las circunstancias relacionadas con la transferencia, y en particular:

- La identificación de la entidad destinataria de la transferencia.
- La naturaleza de los datos que se van a transmitir.
- Las finalidades para las que se transfieran los datos.
- Las medidas de seguridad.
- La duración del tratamiento.
- El país de destino final.
- Las normas sectoriales, o profesionales que pudieran existir.

b) Consentimiento inequívoco del interesado para que sus datos se almacenen en un fichero ubicado en un tercer país o en caso contrario que exista una libre y legítima aceptación de una relación contractual o precontractual en la que el interesado sea parte, y sea necesaria la transferencia para el desarrollo, cumplimiento y control de dicha relación.

c) Que la titularidad del fichero corresponda a una entidad domiciliada en territorio español y que dicha entidad, como responsable del fichero, garantice todas las obligaciones y derechos establecidos, así como que se continúe facilitando desde España los derechos de acceso, rectificación y cancelación.

d) Que en el país de destino los datos no se van a utilizar para fines distintos de los especificados en la inscripción del fichero, así como que no se cederán a terceros sin el consentimiento de los interesados.

Garantías derivadas de cláusulas contractuales apropiadas

La Directiva considera como posibilidad que el responsable del tratamiento sea el que ofrezca las garantías para paliar la insuficiencia del nivel de protección en un tercer país, pudiendo derivarse en cláusulas contractuales apropiadas. Y en su artículo 26.2 se dispone que los estados miembros podrán autorizar una transferencia de datos personales a un tercer país que no garantice un nivel de protección adecuado, cuando el responsable del tratamiento ofrezca garantías suficientes y posibilite el ejercicio de los derechos de acceso, rectificación y cancelación en el país origen de los datos, igualándose en este sentido con el artículo 32 de la LORTAD –hoy artículo 33 de la LOPD.

La primera vez que en la Agencia de Protección de Datos se utilizó la solución contractual en el contexto de la transferencia internacional fue a finales de 1998, habiéndose autorizado 3 transferencias por este sistema en 1999.

Las cláusulas que se venían exigiendo en estos casos con carácter general han sido precisadas y positivadas en la Norma Quinta de la Instrucción 1/2000 de la Agencia de Protección de Datos, a cuyo tenor la autorización será otorgada en caso de que el responsable del fichero aporte un contrato escrito, celebrado entre el transmitente y el destinatario, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

Dada la dicción de la Norma, la vinculación de la Agencia al otorgamiento de la autorización, trata de potenciar la solución contractual, en la línea seguida por el Parlamento Europeo, en su informe de 11 de julio de 2000, que la ha considerado el instrumento más eficaz para garantizar que la transferencia de datos ofrece las garantías adecuadas. También el Documento del Grupo de Trabajo de Protección de Datos al que antes nos

hemos referido, contiene previsiones específicas referidas a esta solución contractual.

Así pues, la autorización será otorgada si se aporta un contrato escrito, en el que la Agencia compruebe que se garanticen los requisitos que se contengan en, al menos, las siguientes menciones:

a) La identificación del transmitente y el destinatario de los datos.

b) La indicación de la finalidad que justifica la transferencia internacional, así como de los datos que son objeto de la transferencia.

c) El compromiso del transmitente de que la recogida y tratamiento de los datos en territorio español respeta íntegramente las normas contenidas en la Ley Orgánica 15/1999 y que el fichero en que se encuentran los datos objeto de la transferencia está inscrito en el Registro General de Protección de Datos o se ha solicitado su inscripción.

d) El compromiso del destinatario de que los datos recibidos serán tratados exclusivamente para la finalidad que motiva la transferencia, así como que procederá a su tratamiento de acuerdo con las normas de protección de datos del derecho español. Asimismo, el destinatario deberá comprometerse a no comunicar los datos a ningún tercero en tanto no haya sido recabado el consentimiento del afectado para ello.

e) Que el destinatario adoptará las medidas de seguridad requeridas por la normativa de protección de datos de carácter personal vigente en España.

f) Que el transmitente y el destinatario responderán solidariamente frente a los particulares, a la Agencia de Protección de Datos y a los Organos Jurisdiccionales españoles por los eventuales incumplimientos del contrato en que pudiera incurrir el receptor, cuando los mismos sean constitutivos de infracción de lo dispuesto en la Ley Orgánica 15/1999 o produzcan un perjuicio a los afectados.

g) Que se indemnizará al afectado que resulte perjudicado como consecuencia del tratamiento efectuado por el destinatario, según el régimen de responsabilidad al que se refiere el apartado anterior.

h) La garantía de que el afectado podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición, tanto ante el transmitente como ante el destinatario de los datos. Asimismo, deberá indicarse que el interesado podrá recabar la tutela de la Agencia de Protección de Datos en los supuestos previstos en la Ley Orgánica 15/1999 en caso de que sus derechos no sean atendidos.

i) El compromiso del destinatario de los datos de autorizar el acceso al establecimiento donde se estén tratando los mismos, así como a la documentación y a los equipos físicos y lógicos, de representantes de la Agencia de Protección de Datos o de la entidad independiente en quien esta delegue, cuando la Agencia lo requiera con el fin de verificar el cumplimiento de las obligaciones derivadas del contrato.

j) La obligación de que, una vez extinguida la relación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transferencia.

k) Que los afectados podrán exigir el cumplimiento de lo estipulado en el contrato en todas aquellas cuestiones en que el mismo les resulte beneficioso.

Referencia al nivel de protección en Estados Unidos. La noción y principios de "Puerto seguro"

Frente al estudio de otros Estados, en los que el punto de partida para el análisis de la cuestión ha sido el estudio de una legislación de protección de datos aplicable en todo el territorio del estado, el problema de partida para el análisis de la cuestión en los Estados Unidos se centra en el hecho de que no existe, dado el marcado carácter autorregulador del comercio en dicho país, una normativa sobre protección de datos de carácter personal aplicable en todo el territorio y en todos los sectores de actividad, sino a lo sumo normas dispersas aplicables a sectores muy concretos.

En efecto, la protección de la intimidad y de los datos en Estados Unidos se enmarca en un complejo entramado de regulación sectorial, tanto en el nivel federal como en el estatal, que se combina con la autorregulación industrial. En este sentido, el Grupo de trabajo ha considerado que este conjunto de leyes sectoriales muy segmentadas y la autorregula-

ción voluntaria no son suficientes para proporcionar protección adecuada en todos los casos a los datos personales transferidos desde la Unión Europea.

A fin de superar los problemas derivados de esta dispersión normativa, el Departamento de Comercio de los Estados Unidos presentó, como documento para la discusión entre las autoridades norteamericanas y de la Unión Europea un borrador de "principios de puerto seguro", a fin de garantizar a los operadores que se adhirieran a los mismos una "presunción de adecuación" al nivel de protección exigido por la Directiva, permitiéndose así la libre transferencia internacional de datos a dichos operadores. Para ello, los operadores debían manifestar ante la Oficina Federal de Comercio (u otra entidad por ella designada) su adhesión a estos principios y su compromiso de llevarlos a la práctica, adoptando para ello las medidas adecuadas.

El Grupo de Trabajo manifestó su opinión en el Dictamen 1/99. A lo largo de 1999, y a partir de la opinión manifestada en este Dictamen, se sometieron al parecer del Grupo de Trabajo cuatro versiones de los citados principios de "puerto seguro", dictándose otros tantos documentos por parte del Grupo, en que se manifestaron aquellos aspectos de los mismos que se consideraron insuficientes frente al nivel de protección mínimo requerido para que pudiera considerarse posible recomendar una decisión afirmativa a la Comisión Europea.

En el último dictamen aprobado durante el año 1999 (dictamen 7/99, relativo al nivel de protección de datos previsto por los principios de «puerto seguro» hechos públicos, junto con las preguntas más frecuentes y otros documentos relacionados, el 15 y 16 de noviembre de 1999 por el Departamento de Comercio de los EEUU), aprobado el 3 de diciembre de 1999, el Grupo de Trabajo consideró que los acuerdos de «puerto seguro» propuestos, tal como quedaban reflejados en las versiones de los diversos documentos, continuaban siendo insatisfactorios, invitando a la Comisión a instar a la parte estadounidense a realizar una serie de mejoras clave.

Finalmente, tras dictaminar (27) sobre el diálogo entre la Unión Europea y los EEUU acerca del Acuerdo de "puerto seguro" y sobre el nivel de protección que proporcionan los principios de puerto seguro, la Comisión emitió su Decisión 2000/520 (28), a cuyo tenor se considerará que garantizan un nivel adecuado de protección los principios de puerto seguro, que seguidamente relacionaremos, interpretados y aplicados de conformidad con la relación de las preguntas más frecuentes (FAQ) publicadas por el Departamento de Comercio de EEUU, con fecha 21 de julio de 2000, que se acompañan como Anexo a la Decisión.

Condiciones de cada transferencia.

Para que los principios de puerto seguro se puedan dar por operativos, en cada transferencia de datos deberán cumplirse las siguientes condiciones:

1. La entidad receptora de los datos deberá haber manifestado de forma inequívoca y pública su compromiso de cumplir los principios aplicados de conformidad con las FAQ.
2. La entidad estará sujeta a la jurisdicción de la Comisión Federal de Comercio o el Departamento de Transporte, organismos públicos estadounidenses que estarán facultados para investigar las quejas que se presenten y solicitar medidas provisionales contra las prácticas desleales o fraudulentas, así como las reparaciones a los particulares independientemente de su país de residencia o nacionalidad, en caso de incumplimiento de los principios y de su aplicación de conformidad a las FAQ, y a los que la Unión Europea reconoce la competencia.
3. La fecha a partir de la cual comenzará a computarse el reconocimiento a un entidad su inclusión en el puerto seguro, será la de la notificación al Departamento de Comercio de los Estados Unidos de su autocertificación de adhesión a los principios y a su aplicación de conformidad con las FAQ, así como de la identidad de uno de los organismos anteriores.

Principios de "Puerto seguro".

1. NOTIFICACION: Las entidades informarán a los particulares de los fines con los cuales recogen y utilizan información sobre ellos; la forma de contactar con ellas para cualquier pregunta o queja; los tipos de terceros a los cuales se revelará la información; las opciones

y medios que la entidad ofrece a los particulares para limitar el uso y su divulgación.

Principio que se corresponde con el *derecho de información* del afectado reconocido en el artículo 5 de la LOPD.

2. OPCION: Las entidades ofrecerán a los particulares la posibilidad de decidir si su información personal puede divulgarse a un tercero o puede usarse para un fin incompatible con el objetivo inicial con el que fue recogida o no haya sido autorizado posteriormente por el particular.

Si se trata de información delicada –noción con la que se alude a los datos calificados de especialmente protegidos en los artículos 7 y 8 de la LOPD– la opción será afirmativa o explícita si la información va a revelarse a un tercero o a utilizarse para un fin distinto del que inicialmente motivó la recogida de la información o de una manera distinta a la autorizada con posterioridad por éste al optar por la aceptación.

En cualquier caso, una entidad debe tratar como delicada toda información recibida de un tercero cuando dicho tercero la identifique y trate como información delicada. Es decir, mediante este principio se consagra el derecho al consentimiento del afectado, del que se excluye el consentimiento tácito cuando los datos son especialmente sensibles, por disposición legal o por haberlos así calificados el interesado.

3. TRANSFERENCIA ULTERIOR: Para revelar información a terceros, las entidades deberán aplicar los principios de notificación y opción. Cuando una entidad desee transferir los datos a un tercero que actúa como agente, podrá hacerlo si previamente se asegura que éste suscribe los principios, si es objeto de una resolución sobre su adecuación con arreglo a la Directiva u otra disposición o si firma con el un Convenio por escrito para que ofrezca como mínimo el mismo nivel de protección de la vida privada que el requerido por dichos principios.

Mediante este principio se acogen las garantías que para el acceso a los datos exige el artículo 12 de la LOPD, evitando que, mediante la utilización de este procedimiento, puedan vulnerarse los principios de protección.

4. SEGURIDAD: Las entidades que creen, mantengan, utilicen o difundan información personal tomarán precauciones razonables para evitar su pérdida, su mal uso y consulta no autorizada, su divulgación, modificación o destrucción, lo que se corresponde con la obligación de tomar las precauciones de índole técnica y organizativas que requiere el artículo 9 de la LOPD.

5. INTEGRIDAD DE LOS DATOS: De acuerdo con los principios, la información personal debe ser pertinente para los fines con los que se utiliza. Una entidad no podrá tratar la información personal de manera incompatible con los fines que motivaron su recogida o aprobó posteriormente el particular. En la medida necesaria para alcanzar dichos fines, las entidades adoptarán medidas razonables para que los datos tengan fiabilidad para el uso previsto y sean exactos, completos y actuales.

De este modo se reconocen los *principios de calidad de los datos* que desde el Convenio 108, artículo 5, se vienen de forma constante requiriendo para el tratamiento de los datos.

6 ACCESO: Los particulares deberán tener acceso a la información personal que las entidades tengan sobre ellos y poder corregir, modificar o suprimir dicha información si resultase inexacta, excepto en dos casos: cuando permitir el acceso suponga una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conlleve para la vida privada de la persona; o cuando puedan vulnerarse los derechos de otras personas.

Con ello, se hacen operativos los *derechos de acceso, rectificación y cancelación* reconocidos en los artículos 15 y 16 de la LOPD. Sin embargo, las condiciones, procedimientos y supuestos de denegación que se recogen en las FAQ, a nuestro juicio, tendrán que ser objeto de particular seguimiento por las autoridades de control, toda vez que, así como en los anteriores principios se tiende a garantizar un nivel de protección equiparable, o incluso una protección más amplia que la recogida en la Directiva 95/46, en estos derechos fundamentales, tal protección puede rebajar el umbral de garantías que estos derechos confieren al interesado.

7. APLICACION: Una protección eficaz de la vida privada debe incluir mecanismos para

garantizar la conformidad con los principios, una vía de recurso para las personas a que se refieren los datos y se vean afectadas por el incumplimiento de dichos principios y sanciones contra la entidad incumplidora. Como mínimo, tales mecanismos deben incluir:

- Una vía de recurso independiente, asequible e inmediatamente disponible para investigar y resolver con arreglo a los principios las denuncias y litigios de los particulares y otorgar daños y perjuicios donde determinen la legislación aplicable o las iniciativas del sector privado.
- Procedimientos de seguimiento para comprobar que los certificados y las declaraciones de las empresas sobre sus prácticas en materia de vida privada se ajustan a la verdad y que dichas prácticas se aplican en consecuencia.
- Obligación de subsanar los problemas derivados del incumplimiento de los principios para las entidades que se hayan adherido a ellos y las sanciones correspondientes contra ellas, que serán lo suficientemente rigurosas para garantizar su cumplimiento.

Con ello, nuevamente se reconocen el haz de facultades que se integran en el contenido esencial del derecho fundamental a la protección de datos, configurándose estas facultades como verdaderos derechos subjetivos cuyo desconocimiento hace irreconocible y por tanto vulnera este derecho fundamental de reciente consolidación.

A contribuir a su divulgación y mostrar la sensibilidad de la Guardia Civil ante él responde la intención del presente artículo.

NOTAS

(1) Cfr. Carta 4487/00, de Derechos Fundamentales de la Unión Europea, 28 de septiembre de 2000, adoptada en la Cumbre de Niza de diciembre de 2000, www.europa.eu.int/comm/justice_home/unit/charte/pdf/charter_fr.pdf artículo 7, respeto de la vida privada y familiar: Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

(2) La traducción es nuestra.

(3) Cfr. Pérez Luño, Antonio Enrique, "Del Habeas Corpus al Habeas Data", *Revista de Informática y Derecho*, 1 (1992), 156.

(4) Cfr. Martín-Casallo López, Juan José, *"La protección de datos personales. Aspectos penales de la cesión de datos"* Servicio de formación continuada. Escuela Judicial, Madrid, 3, 4 y 5 de abril de 2000, documentación de curso CU0036, pág. 5.

(5) Cfr. Carrascosa López, Valentín, "Derecho a la Intimidad e Informática", *Revista de Informática y Derecho*, 1 (1992), 22.

(6) Cfr. Lucas Murillo de la Cueva, Pablo, "Las funciones de la Agencia de Protección de Datos" *Jornadas sobre el Derecho español de la protección de datos personales" Agencia de Protección de Datos* (1996), 265.

(7) Cfr. Lucas Murillo de la Cueva, Pablo, *El derecho a la autodeterminación informativa. La protección de los datos personales frente al uso de la informática*, Madrid: Tecnos Temas clave de la Constitución Española, 1990, pág. 193.

(8) Cfr. Heredero Higueras, Manuel, "La Agencia de Protección de Datos", *Revista de Informática y Derecho*, 6 y 7 (1994), 323.

(9) Cfr. Lucas Murillo de la Cueva, Pablo, *El derecho a la autodeterminación informativa...* pág. 194.

(10) Cfr. Pérez Luño, Antonio Enrique, "Del Habeas Corpus... pág. 159.

(11) Cfr. Heredero Higueras, Manuel, "La Agencia de Protección ... pág 325.

(12) Cfr. Heredero Higueras, Manuel, "La Agencia de Protección ... pág 326.

(13) Cfr. Ull Pont, Eugenio, "Protección de Datos Personales en Ficheros de Titularidad Pública" *Revista iberoamericana de derecho informático*, 19, 20, 21 y 22 (1998), 267.

(14) Cfr. Heredero Higueras, Manuel, "La Agencia de Protección ... pág 330.

(15) Cfr. Martín-Casallo López, Juan José, "La Directiva 95/46CE y su incidencia en el ordenamiento jurídico español" *Jornadas sobre el Derecho español de la protección de datos personales" Agencia de Protección de Datos* (1996), 13.

(16) Cfr. López Ramón, Fernando "La Agencia de Protección de Datos como administración independiente en el derecho español y comunitario europeo" *Jornadas sobre el Derecho español de la protección de datos personales" Agencia de Protección de Datos* (1996), 255.

(17) Sentencia del Tribunal Constitucional 290/2000 de 30 de noviembre de 2000 FJ 8º.

(18) Cfr. Del Peso Navarro, Emilio, *"Ley de Protección de Datos. La nueva LORTAD"* Madrid: Díaz de Santos., 2000, págs. 193-199.

(19) Cfr. Carrascosa López, Valentín, "La LORTAD. Una necesidad en el panorama legislativo español", Revista de Informática y Derecho, 6 y 7 (1994), 62.

(20) Cfr. Rebollo Delgado, Lucrecio, "El derecho fundamental a la intimidad", Madrid: Dikinson, 2000, pág. 249.

(21) Cfr. Aparicio Salom, Javier, "Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal", Navarra: Aranzadi, 2000, pág. 142.

(22) Cfr. Aparicio Salom, Javier, "Estudio sobre la Ley Orgánica..." pág. 144.

(23) Cfr. Decisiones de la Comisión 518 y 519/2000 de 26 de julio de 2000, DOCE nº L 215, 25 de agosto de 2000.

(24) Cfr. Aparicio Salom, Javier, "Estudio sobre la Ley Orgánica..." pág. 185.

(24) Cfr. Instrucción 1/2000 de 1 de diciembre de 2000 de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos, que en su Norma Segunda recuerdael derecho de información del afectado, y las correlativas obligaciones del responsable del fichero, recogidas en el artículo 5 de la LOPD. Igualmente el Título III recuerda el principio general referente al necesario cumplimiento de la LOPD por parte de quienes pretendan efectuar una transferencia internacional de datos.

(26) Cfr. Memoria de la Agencia de Protección de Datos 1999, pág 100.

(27) Cfr. Dictámenes 3/2000 sobre el diálogo entre la Unión Europea y los EEUU acerca del Acuerdo de "puerto seguro" y 4/2000 sobre el nivel de protección que proporcionan los principios de puerto seguro.

(28) Cfr. Decisión de la Comisión de 26 de julio de 2000, con arreglo a la Directiva 95/46 sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, DOCE número L 215 de 25 de agosto de 2000.

BIBLIOGRAFIA

Aparicio Salom, Javier, "Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal", Navarra: Aranzadi, 2000.

Carrascosa López, Valentín, "Derecho a la Intimidad e Informática", *Revista de Informática y Derecho*, 1992.

Carrascosa López, Valentín, "La LORTAD. Una necesidad en el panorama legislativo español", *Revista de Informática y Derecho*, 6 y 7, 1994.

Del Peso Navarro, Emilio, "*Ley de Protección de Datos. La nueva LORTAD*", Madrid: Díaz de Santos, 2000.

Heredero Higueras, Manuel, "La Agencia de Protección de Datos", *Revista de Informática y Derecho*, 6 y 7, 1994.

López Ramón, Fernando, "La Agencia de Protección de Datos como administración independiente en el derecho español y comunitario europeo" *Jornadas sobre el Derecho español de la protección de datos personales, Agencia de Protección de Datos*, 1996.

Lucas Murillo de la Cueva, Pablo, *El derecho a la autodeterminación informativa. La protección de los datos personales frente al uso de la informática*, Madrid: Tecnos Temas clave de la Constitución Española, 1990.

Lucas Murillo de la Cueva, Pablo, "Las funciones de la Agencia de Protección de Datos" *Jornadas sobre el Derecho español de la protección de datos personales, Agencia de Protección de Datos*, 1996.

Martín-Casallo López, Juan José, "*La protección de datos personales. Aspectos penales de la cesión de datos*". Servicio de formación continuada. Escuela Judicial, Madrid, 3, 4 y 5 de abril de 2000, documentación de curso CU0036.

Martín-Casallo López, Juan José, "La Directiva 95/46CE y su incidencia en el ordenamiento jurídico español" *Jornadas sobre el Derecho español de la protección de datos personales, Agencia de Protección de Datos*, 1996.

Pérez Luño, Antonio Enrique, "Del Habeas Corpus al Habeas Data", *Revista de Informática y Derecho*, 1992.

Rebollo Delgado, Lucrecio, "El derecho fundamental a la intimidad", Madrid: Dikinson, 2000.

Ull Pont, Eugenio, "Protección de Datos Personales en Ficheros de Titularidad Pública", *Revista iberoamericana de derecho informático*, 19, 20, 21 y 22, 1998.