Algunas consideraciones sobre el procedimiento sancionador en el ámbito de la protección de datos personales

Eduardo Calvo Rojas

SUMARIO: I. Explicación preliminar.—Parte I: II. Aspectos subjetivos. Los que intervienen en el procedimiento sancionador.—III. Principios y garantías del proceso penal.—IV. Algunas cuestiones de procedimiento.—V. Importancia de las definiciones legales. La autoría de las infracciones.—VI. Antijuricidad de las conductas. Tipificación de las infracciones.—VII. Carga de la prueba.—VIII. Culpabilidad: dolo o culpa.—IX. Las sanciones.—Parte II.

I. EXPLICACIÓN PRELIMINAR

El contenido de este breve trabajo tiene una doble procedencia; y como esta dualidad de origen queda reflejada tanto en la sistemática como en el tono de la exposición, me parece obligado ofrecer esta nota aclaratoria.

La *Parte I* es una síntesis de algunas ideas acerca del procedimiento sancionador que expuse informalmente durante el «Curso sobre Protección de Datos de Carácter Personal», que se desarrolló en julio de 2004 en El Escorial, dentro del programa de cursos de verano de la Universidad Complutense de Madrid. No se pretendía allí —y tampoco ahora— hacer un desarrollo prolijo y detallado del procedimiento sancionador ni de los principios que lo inspiran, que, por lo demás, son sustancialmente coincidentes con los de otros ámbitos de la actividad administrativa sancionadora. Se trataba

únicamente de ofrecer un somero enunciado de singularidades y problemas específicos que plantea la puesta en práctica de la potestad sancionadora en materia de protección de datos de carácter personal, ilustrando algunos de los apartados con una breve reseña de pronunciamientos jurisdiccionales[1].

La *Parte II* contiene, en cambio, más valoración y opinión personal que información. En ella se recogen algunas de las consideraciones que expuse en un artículo, publicado en la revista *Jueces para la Democracia. Información y Debate*[2], en el que, sin ignorar los logros alcanzados, se intenta poner de manifiesto las carencias que todavía presenta el sistema de protección de datos personales en el ordenamiento jurídico español.

Así, aunque responden en su origen a finalidades diferentes, creo que ambas partes tienen un cierto carácter complementario; de ahí este intento de ensamblaje que se ofrece en los apartados que siguen.

PARTE I

II. ASPECTOS SUBJETIVOS. LOS QUE INTERVIENEN EN EL PROCEDIMIENTO SANCIONADOR

En lo que se refiere a la Agencia de Protección de Datos cabe decir que, como en toda institución política o administrativa de reciente creación, cobra especial relevancia la figura de la persona o personas que la encarnan en su periodo inicial, pues estos primeros rectores marcan la actividad del órgano en cuestión con una impronta más acusada y perdurable que la que suele producirse en otras instituciones más señeras y, por ello mismo, menos maleables. Pues bien, es obligado señalar que los tres Directores que hasta ahora ha tenido la Agencia de Protección de Datos ofrecen un claro perfil de juristas preocupados por el respeto a las garantías y la pureza del procedimiento, lo que obviamente ha repercutido en la positiva valoración que merecen los expedientes sancionadores de la Agencia en su vertiente procedimental.

---

[1] Cuando se habla aquí de pronunciamientos jurisdiccionales se está haciendo referencia principalmente a los de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, órgano que desde la entrada en vigor de la Ley reguladora de esta jurisdicción de 1998 tiene atribuida la competencia para conocer de los recursos contra las resoluciones de la Agencia de Protección de Datos (Disposición Adicional Cuarta.5 LJCA de 1998). El Tribunal Supremo está resolviendo por el momento recursos de casación relativos a litigios que se rigen por la antigua Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), y, por tanto, apenas ha comenzado a emitir resoluciones directamente referidas a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). No obstante, las sentencias del Tribunal Supremo en este campo marcan una pauta interpretativa que no debe ser ignorada porque entre la legislación que en ellas se aplica y la norma ahora vigente existe una considerable semejanza y porque, además, alguna sentencia del Tribunal Supremo invoca ya como referente normativo los preceptos de la Ley Orgánica 15/1999 aunque no sea ésta la norma aplicable al caso que allí se resuelve (véase como ejemplo la STS, Sala Tercera, Sección 6.ª, de 6 de octubre de 2000).

[2] «La protección de los datos de carácter personal», revista *Jueces para la Democracia. Información y Debate,* n.º 48, noviembre 2003.

Y si de las personas que encarnan la institución pasamos a referirnos a los sujetos «inculpados» en los expedientes sancionadores que tramita la Agencia, debe decirse que abundan, por supuesto, los casos en los que el procedimiento se dirige contra la actuación de entidades financieras, compañías de telecomunicaciones, empresas dedicadas a la gestión y desarrollo de campañas de publicidad o, en fin, entidades dedicadas específicamente a la gestión y comercialización de bases de datos sobre solvencia patrimonial o de cualquier otra índole; y ello es así porque la actividad de estas empresas o grandes corporaciones inevitablemente supone el manejo de ingentes bases de datos, cuando no sucede que la creación y comercialización de estos ficheros de datos personales constituye una parte sustancial de su volumen de negocio. Este contacto habitual y cotidiano con material tan sensible —los datos personales— comporta inevitablemente un mayor riesgo de rozar o sobrepasar los límites de la legalidad. Pero, dado el ámbito de aplicación de la normativa sobre protección de datos de carácter personal, no cabe descartar que el procedimiento se dirija también contra profesionales o ciudadanos particulares. Y, algo sobre lo que luego volveremos, no es infrecuente que el procedimiento tenga por objeto la actuación irregular de entidades públicas y órganos de la Administración.

Por lo demás, la intervención del ciudadano particular en esta clase de procedimientos no es sólo en calidad de posible responsable de la conducta infractora, sino también, y esto es mucho más frecuente, como denunciante o reclamante. En esta vertiente conviene señalar que hoy está ya pacíficamente admitida la legitimación activa del denunciante para promover recurso contencioso-administrativo contra la resolución de la Agencia de Protección de Datos que considere contraria a sus intereses[3]. Y también son ya reiterados los pronunciamientos que declaran que una vez formulada la denuncia el denunciante carece de poder de disposición sobre ella, o, dicho de otra manera, que en materia de protección de datos personales el denunciante no dispone de la acción sancionadora ni tiene potestad para eximir de responsabilidad al denunciado[4].

III. PRINCIPIOS Y GARANTÍAS DEL PROCESO PENAL

Recogiendo la copiosa jurisprudencia del Tribunal Constitucional y del Tribunal Supremo sobre la materia, los pronunciamientos de la Audiencia Nacional vienen declarando que los principios y garantías del Derecho Penal son trasladables a los procedimientos administrativos sancionadores por ser manifestación del *ius puniendi* del Estado (SsTC 18/1981, 29/1989, 58/1989, 22/1990, 120/1994, etc.). No obstante, dadas las diferencias existentes, debe procederse con cautela cuando se trata de llevar al ámbito admi-

[3] Pueden verse, entre otras, las SsAN, 1.ª, de 11 y 18 de mayo de 2001.
[4] SsAN, 1.ª, de 4 de abril de 2002, 8 de noviembre de 2002 y 18 de octubre de 2004.

nistrativo sancionador las garantías del artículo 24.2 de la Constitución en materia de procedimiento, pues la traslación de aquellos principios a la actividad sancionadora de la Administración procederá sólo en la medida necesaria para preservar los valores en los que se basa el mencionado precepto constitucional y que resulten compatibles con la naturaleza del procedimiento sancionador (SsTC 18/1981, 29/1989, 212/1990, 246/1991, 145/1993, 120/1994, 197/1995, 120/1996, 7/1998, 56/1998, etc.)[5].

IV. ALGUNAS CUESTIONES DE PROCEDIMIENTO

En general, ya lo hemos anticipado, se observa en los expedientes sancionadores de la Agencia de Protección de Datos una tramitación cuidada y correcta, en particular si se la compara con procedimientos sancionadores provenientes de otros órganos administrativos de mayor antigüedad y tradición.

Acaso la cuestión procedimental que con mayor frecuencia se invoca se refiere a los problemas que suscita el cómputo de los plazos a efectos de la caducidad del procedimiento (art. 42.2 de la Ley 30/1992), y ello en relación con el uso y el eventual «abuso» por parte de la Agencia de las llamadas «actuaciones previas» en una fase preliminar anterior a la incoación en sentido estricto del procedimiento sancionador. Con carácter general, cabe señalar que la complejidad técnica de los hechos investigados en esta clase de expedientes hace que con frecuencia resulte indicada, e incluso inevitable, esta fase de actuaciones previas; entre otras cosas, porque el artículo 13.1 del Reglamento que regula el ejercicio de la potestad sancionadora, aprobado por Real Decreto 1398/1993, requiere que, entre otras determinaciones, el acuerdo de incoación del procedimiento contenga ya la identificación de la persona contra la que éste se dirige, una exposición sucinta de los hechos, así como la posible calificación jurídica de éstos y la indicación de las sanciones que pueden imponerse. Tales precisiones difícilmente pueden hacerse en muchos casos si antes de la incoación del procedimiento no se han realizado determinadas diligencias de averiguación y comprobación. Aun así, el cómputo de los plazos podrá llevar a declarar la caducidad del procedimiento si llega a constatarse cualquier abuso por parte de la Agencia (por ejemplo, llevando toda la investigación a la fase de «actuaciones previas», de manera que en el momento de la incoación del procedimiento todo está ya definido y perfilado)[6].

Otra cuestión a veces controvertida se refiere a que, en ocasiones, la Agencia de Protección de Datos en el acuerdo de incoación del procedimiento atribuye a los hechos investigados una determinada calificación jurídica que luego modifica en la propuesta de resolución y en la resolución definitiva. En este punto son mayoritarios los pronunciamientos que declaran que tal cambio de calificación a lo largo del procedimiento no constituye una

[5] Una aplicación de esta doctrina puede verse en SAN, 1.ª, de 8 de junio de 2001.
[6] SsAN, 1.ª, de 11 de mayo de 2001 y 8 de noviembre de 2002.

anomalía siempre que se produzca dentro de ciertos límites que, básicamente, consisten en la igualdad sustancial de los hechos y la homogeneidad de la infracción que se imputa[7].

V. IMPORTANCIA DE LAS DEFINICIONES LEGALES. LA AUTORÍA DE LAS INFRACCIONES

Al ser la protección de datos personales una materia cuya regulación legal es relativamente nueva, tienen especial importancia las definiciones de los conceptos más usuales y a la vez más específicos de este ámbito que nos ofrece el artículo 3 de la Ley Orgánica 15/1999 (el propio concepto de *dato de carácter personal*, las nociones de *responsable* y *encargado* del *fichero* o *tratamiento*, y el alcance de expresiones tales como *procedimiento de disociación*, *fuentes accesibles al público*, *comunicación de datos*, etc.).

No obstante, la variada casuística que ofrece la vida real siempre sobrepasa las previsiones del legislador, obliga a una constante labor de reinterpretación de algunos de aquellos conceptos y lleva a abordar cuestiones que la norma no deja resueltas de una manera directa. Así, por ejemplo, la cuestión relativa a si es posible la existencia de «co-responsable» de un fichero o si necesariamente debe estar dilucidado si nos encontramos ante la figura del responsable o la del encargado para que puedan adoptarse determinadas medidas cautelares[8]. En fin, el Tribunal Supremo ha emitido algunos pronunciamientos en los que se ofrece una interpretación sumamente restrictiva de la figura del responsable del fichero (SsTS, Sala Tercera, Sección 6.ª, de 13 de abril y 3 de diciembre de 2002, ambas dictadas resolviendo recursos de casación para la unificación de doctrina); pero, estando referida esa doctrina jurisprudencial a los preceptos y definiciones de la LORTAD de 1992, entiendo que la interpretación que ofrecen esas sentencias no cabe extenderla sin más a las disposiciones de la vigente LOPD de 1999.

VI. ANTIJURICIDAD DE LAS CONDUCTAS. TIPIFICACIÓN DE LAS INFRACCIONES

Tomando la clásica graduación de las infracciones en leves, graves y muy graves (véase el art. 44 de la Ley Orgánica 15/1999 en relación con el art. 129.1 de la Ley 30/1992), la normativa española sobre protección de datos personales aborda la tipificación de las distintas infracciones mediante una remisión a los principios definidos en la propia Ley y relacionados con la calidad y exactitud de los datos (art. 4), el derecho de información en la re-

[7] STC 302/2000, cuya doctrina se recoge en SAN, 1.ª, de 8 de junio de 2001.

[8] Algunas de estas cuestiones pueden verse en las SsAN de 2 de marzo y 21 de septiembre de 2001.

cogida de datos (art. 5) y la exigencia del consentimiento del afectado para el tratamiento de sus datos (art. 6), así como en relación con los preceptos relativos a datos especialmente protegidos (art. 7), seguridad de los datos (art. 9), deber de secreto (art. 10) y necesidad de consentimiento para la cesión de datos a terceros (arts. 11 y 12).

Esta formulación de las infracciones mediante la remisión a diversos principios y garantías cuya vulneración determinaría la existencia de la infracción acaso se explique por la dificultad para definir de una manera más directa las conductas infractoras que podrían producirse. Es, desde luego, una técnica legislativa cuestionable desde el punto de vista de las exigencias del principio de legalidad en su vertiente material, aunque también es cierto, a modo de paliativo, que no nos encontramos aquí ante una remisión a principios innominados y dispersos pues tales principios y garantías quedan debidamente acotados en el Título II del propio texto legal bajo las rúbricas de Principios de la Protección de Datos (arts. 4 a 12) y Derechos de las Personas (arts. 13 a 19)[9].

Por otra parte, la Ley Orgánica 15/1999 ha suprimido algunas de las imprecisiones que estaban presentes en la Ley Orgánica 5/1992. Sirva como ejemplo la distinción que hacía la Ley Orgánica 5/1992 entre la infracción leve, consistente en «no conservar actualizados los datos», y la infracción grave, que consistía en esa misma conducta «cuando resulten afectados los derechos de las personas», dualidad que, además de artificiosa, hacía depender la gravedad de la infracción de la conducta de terceros, lo que planteaba serios problemas a la hora de valorar la culpabilidad del infractor[10]. La Ley Orgánica 15/1999 ha suprimido esta dualidad a base de mantener únicamente el tipo de la infracción grave.

No obstante, subsisten en la Ley Orgánica 15/1999 determinadas imprecisiones. Así, por ejemplo, hay definiciones de conductas infractoras que en buena medida son coincidentes o se solapan, como, por ejemplo, las definidas en los apartados d) y f) del artículo 44.3 (el primero de ellos, ya lo hemos señalado, define como infracción el *tratar o usar los datos* personales conculcando los principios y garantías de la Ley, mientras que en el segundo de los apartados mencionados la conducta infractora consiste en *mantener los datos de carácter personal inexactos*)[11]. Por lo demás, el esfuerzo interpretativo

---

[9] Por todo ello, aun reconociendo que existen fórmulas de definición de infracciones más certeras y precisas que las empleadas en algunos apartados de la Ley Orgánica 15/1999, la Audiencia Nacional ha entendido que la redacción dada al artículo 44.3.d) de la Ley Orgánica 15/1999 (precepto en el que se define como infracción grave la conducta consistente en: «*...Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente ley...*») no es tan genérica o imprecisa como para considerar que no cumple la exigencia constitucional de *predeterminación suficiente del ilícito* tal y como ha sido definida y perfilada en la jurisprudencia constitucional (pueden verse en este sentido las SsAN, 1.ª, de 8 de noviembre de 2002 y 8 de octubre de 2003).

[10] Sobre estas cuestiones pueden verse la STS de 28 de octubre de 2000 y las SsAN de 2 de marzo, 11 de mayo y 25 de mayo de 2001.

[11] Este solapamiento en algunos tipos infractores de la Ley Orgánica 15/1999 es objeto de examen en las SsAN de 8 de noviembre de 2002 y 8 de octubre de 2003. Por otra parte, el mismo fenómeno ya se daba en la Ley Orgánica 5/1992 —arts. 43.3.d) y 43.3.f)— y, en alguna ocasión, la Agencia de Protección de Datos aplicó uno y otro tipo para conductas iguales, como se recoge en la SAN de 29 de noviembre de 2001.

adicional que requieren estas ambigüedades de la normativa aplicable debe abordarse en todo caso «... teniendo en cuenta el carácter restrictivo y nunca expansivo que debe presidir toda acción administrativa sancionadora, incluida, claro es, la regulada en la Ley Orgánica 15/1999, de 13 de diciembre» (SAN, 1.ª, de 16 de marzo de 2004).

Cabe señalar también que la Ley Orgánica 15/1999 trajo consigo la atenuación de algunos tipos. Así, la vulneración del deber de secreto del artículo 10 era infracción grave o muy grave —arts. 43.3.g) y 43.4.g) de la Ley Orgánica 5/1992—, mientras que ahora puede ser también leve —arts. 44.2.e), 44.3.g) y 44.4.g) de la Ley Orgánica 15/1999—, siendo el tipo básico el de la infracción leve[12].

Para terminar este apartado, y dada la proliferación de litigios en los que se suscita controversia en torno a la imposición de sanciones por infracciones consistentes en el tratamiento o la comunicación de datos personales sin el consentimiento del titular, parece oportuno detenernos un momento en este punto.

La regla general establece la necesidad del consentimiento del afectado tanto para el tratamiento y uso de sus datos (art. 6.1 LOPD) como para la comunicación o cesión de éstos a un tercero (art. 11.1 LOPD), aunque en ambos casos la Ley contempla supuestos de dispensa o inexigibilidad del consentimiento. Así, no se requiere el previo consentimiento cuando se trata de datos recabados para el ejercicio de las funciones propias de las Administraciones en el ejercicio de sus competencias; de datos obtenidos en el seno de una relación negocial, laboral o administrativa y sean necesarios para su cumplimiento o realización; cuando sean necesarios para preservar un interés vital (por ejemplo, sanitario), o cuando hayan sido obtenidos de fuentes accesibles al público y su tratamiento sea necesario para fines legítimos, siempre que no se vulneren los derechos y libertades fundamentales del interesado[13]. El enunciado de estos supuestos de excepción o dispensa del consentimiento en el artículo 6.2 LOPD es más riguroso que el de la antigua LORTAD (Ley Orgánica 5/1992) y, en todo caso, la efectividad del derecho a la protección de los datos debe llevar a interpretar aquéllos de manera estricta y nunca extensiva[14].

---

[12] Ante este cambio normativo, la SAN de 17 de enero de 2001 aplica retroactivamente la nueva norma por ser más favorable.

[13] La definición de «fuente accesible al público», que antes no figuraba en norma de rango legal, sino en el artículo 1.3 del Reglamento aprobado por Real Decreto 1332/1994, de 20 de junio, queda ahora recogida en el artículo 3.j) de la LOPD.

[14] La interpretación y el alcance de estos supuestos de excepción, en particular el relativo a datos obtenidos de «fuentes accesibles al público», pueden verse en SsAN de 2 de febrero, 25 de mayo y 29 de noviembre de 2001.

VII. CARGA DE LA PRUEBA

Rige en este ámbito, como es obvio, el derecho a la presunción de inocencia, principio cuya significación y alcance están ya profusamente estudiados desde muy diversas perspectivas y que no reviste perfiles diferentes cuando se trata de infracciones en materia de protección de datos personales.

Ahora bien, la efectividad de aquel derecho no supone que deba recaer sin más sobre la Agencia de Protección de Datos la carga de acreditar todos y cada uno de los elementos que integran el hecho infractor, pues rige también en este ámbito el principio de «disponibilidad de la prueba». Así, cuando se imputa a alguien el haber realizado un tratamiento de datos personales sin el consentimiento del afectado o no haber atendido un determinado requerimiento, es claro que incumbe a la Administración identificar los datos personales indebidamente utilizados y acreditar el tratamiento que se ha hecho de ellos; pero si la persona o entidad contra la que se dirige el procedimiento sancionador alega un hecho con el que pretende justificar su actuación o excluir su responsabilidad (por ejemplo, alega haber recabado el consentimiento o haber respondido en forma debida al requerimiento), la prueba de estos extremos corresponderá a quien los alega[15].

VIII. CULPABILIDAD: DOLO O CULPA

Conforme al régimen general de la culpabilidad en las infracciones administrativas (art. 130 Ley 30/1992), en materia de protección de datos se puede incurrir en responsabilidad infractora tanto de manera intencionada o dolosa como por descuido, negligencia o a título de simple inobservancia[16]. Ahora bien, teniendo en cuenta el carácter restrictivo y nunca expansivo que debe presidir toda actuación sancionadora, como *última ratio* de la acción administrativa, este reconocimiento de que se puede incurrir en infracción por mera negligencia no debe conducir a que, mediante una interpretación forzada y rigorista de la legislación sobre protección de datos personales, se llegue a la conclusión, sin duda desproporcionada, de que todo error, por nimio que sea, en el manejo de cualquier dato —por ejemplo, un simple error de anotación en una cuenta bancaria— ha de ser considerado como una infracción grave de la LOPD[17].

Por otra parte, el Tribunal Supremo tiene declarado que *«… aunque la culpabilidad de la conducta debe también ser objeto de prueba debe considerarse, en orden a la asunción de la correspondiente carga, que ordinariamente los elementos volitivos y cognoscitivos necesarios para apreciar aquélla forman parte de la conducta típica probada, y que su exclusión requiere que se acredite la ausen-*

[15] SAN, 1.ª, de 17 de junio de 2001.
[16] SsAN, 1.ª, de 25 de mayo de 2001 y 8 de octubre de 2003, entre otras.
[17] SAN, 1.ª, de 17 de marzo de 2004.

cia de tales elementos, o en su vertiente normativa, que se ha empleado la diligencia que era exigible por quien aduce su inexistencia; no basta, en suma, para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa»[18].

En fin, recuérdese que, como ya quedó señalado, en materia de protección de datos personales el denunciante no dispone de la acción sancionadora ni tiene potestad para eximir de responsabilidad al denunciado[19].

IX. LAS SANCIONES

Dado el importe comparativamente elevado de las sanciones previstas en la LOPD[20], adquiere aquí especial relevancia la adecuada toma en consideración del principio de proporcionalidad, que, por lo demás, es de inexcusable observancia en cualquier ámbito sancionador[21].

En relación con lo anterior, en materia de protección de datos personales es frecuente que los inculpados en procedimientos sancionadores soliciten que se les aplique la reducción de la sanción prevista en el artículo 45.5 LOPD[22]; pero esta especial atenuación de la multa sólo procede cuando haya quedado acreditada la concurrencia de circunstancias que lleven a apreciar *una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho*.

Más adelante haremos algunas consideraciones sobre el régimen de sanciones de la LOPD. Por el momento, nos limitaremos a dejar reseñado que cuando el procedimiento sancionador se dirige contra una Administración Pública queda excluida la posibilidad de sanciones económicas; en tales casos, el Director de la Agencia debe indicar en su resolución las medidas que deben adoptarse para que cesen o se corrijan los efectos de la infracción y, en su caso, proponer la iniciación de actuaciones disciplinarias, comunicando todo ello al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados, si los hubiera, así como al Defensor del Pueblo (art. 46 LOPD).

---

[18] STS de 23 de enero de 1998.

[19] Pueden verse en este sentido las ya citadas SsAN, 1.ª, de 4 de abril de 2002, 8 de noviembre de 2002 y 18 de octubre de 2004.

[20] De 100.000 a 10.000.000 de pesetas para las infracciones leves; de 10.000.000 a 50.000.000 de pesetas para las graves, y de 50.000.000 a 100.000.000 de pesetas para la infracciones muy graves (art. 45 LOPD).

[21] En consonancia con lo previsto en el artículo 130 de la Ley 30/1992, el artículo 45.4 LOPD establece que la cuantía de la sanción a imponer en cada caso *«... se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de tratamientos afectados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados (...) y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora»*.

[22] Este precepto contempla la posibilidad de aplicar la escala de sanciones prevista para las infracciones de grado inferior al de la que se examina; es decir, permite sancionar una infracción muy grave como si fuera grave y sancionar una infracción grave como si fuera leve.

PARTE II

I. Parece algo tópica la afirmación de que cuando el legislador aborda la regulación de una materia que considera necesitada de control suele recrearse estableciendo unos mecanismos de intervención aparentemente muy bien perfilados pero que luego la Administración no está en condiciones de poner en práctica, bien por falta de recursos adecuados, bien, sencillamente, por falta del impulso necesario para su plena efectividad. Sin embargo, en este caso el tópico no es enteramente certero pues uno de los principales logros de la normativa española ha consistido en la configuración de un órgano específico e independiente, la Agencia de Protección de Datos, que desde su origen viene desarrollando una labor destacable no sólo en aquellos aspectos más plásticos y visibles de su actuación (actividad inspectora y sancionadora), sino en otras facetas más calladas y difusas como las relacionadas con la divulgación, la elaboración de instrucciones sobre modos de proceder tanto en el sector privado como en el público y, en fin, la tarea de persuadir a todos sobre el inexcusable deber de prestar la debida protección a un derecho fundamental del que muchos no tienen siquiera conciencia de que exista.

Así, la normativa española sobre protección de datos de carácter personal parece cumplir, en principio, los requisitos necesarios para su efectividad; y ello puede decirse tanto de la ya derogada Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), como de la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

Centrándonos ahora en esta última norma, es fácil comprobar que la LOPD de 1999 incorpora en su artículo 3 las *definiciones* de los términos más específicos de la materia que se regula (datos de carácter personal, fichero, tratamiento de datos, responsable del fichero, encargado del fichero, procedimiento de disociación, cesión o comunicación de datos, fuentes accesibles al público,...); determina el *objetivo y el ámbito de aplicación de la Ley,* dejando referido éste «*... a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado*» (art. 2.1 LOPD); establece en sus artículos 4 a 12 los *principios de la protección de datos* (calidad de los datos, derecho de información, consentimiento del afectado, seguridad de los datos, deber de secreto y acceso a los datos por cuenta de terceros, con singular atención a determinados datos especialmente protegidos); encomienda a un ente público independiente, la *Agencia de Protección de Datos*[23], la gestión y fiscalización del cumplimiento de la normativa, así como la tarea de orientar la actuación en este ámbito tanto de los particulares como de las Administraciones; y se establecen en la LOPD una serie de cauces o *mecanis-*

[23] Bajo la vigencia de la antigua Ley Orgánica 5/1992 se aprobó el Estatuto de la Agencia de Protección de Datos por Real Decreto 428/1993, de 26 de marzo (*BOE* n.º 106, de 4 de mayo de 1993), cuya vigencia fue mantenida por la Disposición Transitoria Tercera de la Ley Orgánica 15/1999.

mos de actuación como son el Registro General de ficheros de datos (art. 39), la potestad de inspección (art. 40), la potestad sancionadora (arts. 43 a 49) y la potestad de gestión, incluyéndose en esta última la recepción de quejas y reclamaciones y el suministro de información, así como la función orientadora, que se canaliza a través de instrucciones, interpelaciones y consultas[24].

A todo ello cabe añadir que, al menos en lo que se refiere a su configuración constitucional, la protección que nuestro ordenamiento ha querido dispensar a los datos de carácter personal encuentra un innegable respaldo tanto en las resoluciones del Tribunal Europeo de Derechos Humanos[25] como en las del Tribunal Constitucional español[26]. Entre los pronunciamientos de este último es obligado destacar la doctrina contenida en la STC 292/2000, de 30 de noviembre (*BOE* de 4 de enero de 2001), que define y delimita el derecho a la protección de datos personales del artículo 18.4 de la Constitución como un derecho fundamental autónomo y distinto de los derechos al honor y a la intimidad personal reconocidos y amparados en el artículo 18.1 del propio texto constitucional.

Pero todo ese entramado normativo e institucional —incluido el marchamo de rango constitucional— no ha logrado impedir que el ciudadano bien informado tenga la fundada percepción de que sus datos de carácter personal distan mucho de estar debidamente protegidos. A diario recibimos en nuestros domicilios envíos publicitarios en los que figuran datos personales que nosotros no hemos facilitado a la empresa anunciante; también es frecuente que entidades con las que mantuvimos hace años cualquier relación comercial nos sigan acosando con mensajes y recordatorios, como si sus sistemas informáticos, más que una extensa memoria, tuviesen un profundo rencor. Muchos ciudadanos han pasado por una desagradable experiencia al constatar que un incidente de morosidad con una determinada oficina bancaria en el que habían incurrido años atrás y que ya quedó en su día solventado sigue, sin embargo, reflejado mucho tiempo después en un «fichero de morosos» que les cierra las puertas a cualquier solicitud de crédito ulterior, con la misma o con cualquier otra entidad financiera. De cuando en cuando,

---

[24] Son muestra de esta labor normativa y didáctica de la Agencia de Protección de Datos sus instrucciones relativas a prestación de servicios de información sobre solvencia patrimonial y crédito (Instrucción 1/1995, de 1 de marzo); sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario (Instrucción 2/1995, de 4 de mayo); sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios (Instrucción 1/1996, de 1 de marzo); sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo (Instrucción 2/1996, de 1 de marzo); la relativa al ejercicio de los derechos de acceso, rectificación y cancelación (Instrucción 1/1998, de 19 de enero); o la relativa a las normas por las que se rigen los movimientos internacionales de datos (Instrucción 1/2000, de 1 de diciembre). Debe notarse que esta última Instrucción 1/2000 fue impugnada en vía jurisdiccional y parcialmente anulada por sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, Sección 1.ª, de 15 de marzo de 2002 (Recurso 271/01).

[25] Pueden verse, entre otras, las SsTEDH caso *Laender*, de 26 de marzo de 1987; caso *Z contra el Reino Unido,* de 25 de febrero de 1997; caso *Funke contra Francia*, de 25 de febrero de 1993.

[26] SsTC 110/1984; 154/1988; 254/1993, de 20 de julio; 143/1994, de 9 de mayo; 11/1998; 94/1998; 144/1999, y 290/2000.

la prensa nos da noticias sobre el abandono en papeleras y contendores, o directamente en la vía pública, de documentos o listados que contienen datos personales y reservados provenientes de bancos, empresas, hospitales, etc. En fin, ni siquiera aquellos datos a los que nuestra legislación quiere dispensar una especial protección (los que revelan la ideología, la militancia política o sindical, la orientación sexual, las creencias religiosas y los relativos a la salud) están libres de graves agresiones que se producen por descuido o de manera intencionada en el ámbito de las relaciones empresariales, laborales o comerciales. Y como prueba de que no se trata aquí de exagerar, baste decir que todos los ejemplos enunciados, y algunos que volveremos a mencionar, están tomados de casos reales que han sido objeto de expedientes en la Agencia de Protección de Datos y de ulteriores recursos en vía jurisdiccional.

En los párrafos que siguen trataremos de aportar algunas notas que quizá ayuden a explicar que, pese a los logros alcanzados, nada desdeñables, la tarea para alcanzar una efectiva protección de los datos personales está apenas iniciada.

II. Si tomamos como referencia el Convenio del Consejo de Europa de 1981[27] y la Directiva 95/46/CE, de 24 de octubre de 1995[28], podemos afirmar que la regulación contenida en nuestra LOPD de 1999 recoge de manera acertada los criterios que marca la normativa comunitaria y, en algunos aspectos, la legislación española vigente establece unos mecanismos de protección más enérgicos que los que propugna aquélla[29]. Y aunque la normativa comunitaria no fija criterios para la determinación de las sanciones, dejando este aspecto de la regulación para su concreción por cada Estado miembro, bien puede decirse que también en este punto la legislación española ha adoptado posiciones avanzadas al establecer un abanico de sanciones económicas considerablemente severas. Por ello cabe señalar que si el régimen sancionador inserto en nuestra legislación sobre protección de datos personales presenta un flanco débil, no es por la cuantía de las multas, sino más bien por el lado de la tipificación de las infracciones, vertiente ésta que incurre en demasiadas generalidades e imprecisiones[30].

---

[27] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.

[28] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*.

[29] En realidad, las pautas que establece la Directiva 95/46/CE estaban en buena medida anticipadas en la Ley Orgánica 5/1992, de 29 de octubre.

[30] En el catálogo de infracciones que recoge el artículo 44 LOPD se incluyen tipificaciones tan poco precisas como las que se refieren a conductas consistentes en: «tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo...» —art. 44.3.d) LOPD—; «tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o atente contra el ejercicio de derechos fundamentales» —art. 44.4.f)—; o la que tipifica como infracción «la obstrucción al ejercicio de la función inspectora» —art. 44.3.j)—.

Pese a todo, no son los defectos de regulación —que los hay—, sino factores de otra índole, los que determinan que la legislación sobre protección de datos personales no haya dado aún todo el fruto que de ella cabía esperar. Así, la generalizada falta de información sobre la existencia misma de este «derecho fundamental a la protección de los datos personales», reconocido como tal en la STC 292/2000, acaso constituye la causa más determinante de que los mecanismos de protección habilitados en la LOPD de 1999 no hayan desplegado todos sus efectos.

Los ciudadanos se muestran todavía escasamente beligerantes en la defensa de este derecho fundamental de nuevo cuño. De otro modo no se explica el número relativamente bajo de denuncias que se formulan ante la Agencia de Protección de Datos frente al masivo cúmulo de infracciones de las que somos testigos o víctimas casi a diario. Así, sin necesidad de acudir a ejemplos que han tenido trascendencia en los medios de comunicación, cada vez que recibimos un envío publicitario personalizado remitido por alguien a quien no hemos facilitado nuestros datos estamos en presencia de una posible infracción grave o muy grave por tratamiento o cesión inconsentidos de datos de carácter personal; también hay materia para investigar una posible vulneración de derechos cuando la anotación en un fichero de morosos es inexacta o se prolonga en el tiempo después de que el deudor haya regularizado su situación, cuando un colegio profesional o una empresa ceden a un tercero sus listas de colegiados o de clientes sin el consentimiento de éstos, o cuando una base de datos o un determinado fichero incorporan datos personales sin justificar su procedencia y sin acreditar que provengan de fuentes accesibles al público[31]. Y, sin embargo, no sólo no se produce un número de denuncias medianamente proporcionado al cúmulo de infracciones potenciales, sino que en la mayoría de los casos el ciudadano afectado ni siquiera es consciente de que pueda haber existido una vulneración de sus derechos.

Esta falta de concienciación resulta especialmente llamativa cuando se constata que una parte significativa de los procedimientos tramitados por irregularidades o vulneraciones en la protección de datos de carácter personal vienen motivados por la actuación de entidades y órganos administrativos —singularmente de la Administración Local— y de otras corporaciones de Derecho Público[32], siendo así que todas estas entidades integradas en el

---

[31] Ya hemos hecho referencia a que, según lo dispuesto en los artículos 6.2 y 11.2.b) de la LOPD, no resulta necesario el consentimiento de los afectados para el tratamiento y cesión de sus datos personales cuando tales datos hayan sido recogidos de una fuente accesible al público, encargándose la propia ley de definir lo que se entiende por *fuentes accesibles al público* —art. 3.j) LOPD—. Ahora bien, como la mayoría de los que se ven sorprendidos manejando ficheros de datos cuya procedencia no ha quedado debidamente justificada alegan en su defensa que los han obtenido de fuentes accesibles al público, tanto en las resoluciones de la Agencia de Protección de Datos como en las sentencias de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional existe una variada gama de pronunciamientos en los que se aplica e interpreta aquella definición legal. Sirvan de muestra las SsAN, 1.ª, de 29 de noviembre de 2001, 10 de enero de 2002 y 22 de noviembre de 2002.

[32] Durante el año 2002, la Agencia de Protección de Datos de la Comunidad de Madrid expedientó a 48 instituciones públicas (ayuntamientos, colegios, centros deportivos...) por conductas irregulares en el manejo de ficheros de datos personales. Información publicada en el periódico *El País* de 8 de abril de 2003.

sector público están igualmente sujetas a las disposiciones de la Ley Orgánica 15/1999, aunque con las particularidades que la propia norma establece, y que, colocándonos en una posición deliberadamente ingenua, de los entes públicos debe siempre esperarse un plus de diligencia en todo lo relativo a la protección de los derechos fundamentales.

Cabe mencionar dos circunstancias que, sin duda, favorecen estas carencias que venimos señalando, tanto la falta de efectividad en la protección como la escasa beligerancia en la defensa del propio derecho. De un lado, si antes hemos señalado que la LOPD contiene un elenco de sanciones económicas de considerable cuantía, también hemos indicado que ninguna de éstas puede imponerse cuando el responsable de la infracción es una Administración Pública, pues en tal caso el artículo 46 LOPD (y lo mismo sucedía con el art. 45 de la antigua LORTAD) excluye la sanción económica y limita el alcance de la resolución a que por parte del Director de la Agencia de Protección de Datos se establezcan las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción y, en su caso, se proponga la iniciación de actuaciones disciplinarias contra la autoridad o funcionario responsable[33]. Pues bien, aunque a algunos puede parecer un gesto prudente esta decisión del legislador de excluir las sanciones económicas cuando el infractor es una Administración Pública, debe notarse que este trato privilegiado no deriva de una exigencia constitucional ni es consustancial al juego de las relaciones interadministrativas y, de hecho, no existe esa misma cautela o deferencia en otros ámbitos de la acción administrativa[34]. Todo indica que el legislador ha sido consciente de que el incumplimiento era (y es) masivo en este ámbito, y muy particularmente destacada la falta de cumplimiento por parte de las Administraciones Públicas, y ha preferido seguir respecto de éstas la vía de la persuasión para la paulatina implantación de nuevos modos de actuar en materia de protección de datos.

En esa misma línea, y ésta es la segunda de las circunstancias a que antes aludíamos, cabe señalar que, junto a un plazo razonable de tres años que la vigente Ley Orgánica 15/1999 estableció para que «los ficheros y tratamientos automatizados» preexistentes se adecuasen a sus determinaciones (Disposición Adicional Primera LOPD), la propia norma estableció un periodo mucho más amplio, nada menos que doce años a contar desde el 24 de octubre de 1995, para la adecuación de los «ficheros y tratamientos no automatizados». El amplísimo periodo de tiempo al que se extiende esta moratoria —que no concluirá hasta finales del año 2007— puede ser considerado como una muestra de

[33] Aparte de esta singularidad en materia sancionadora, la LOPD de 1999 contiene una serie de normas específicas sobre ficheros de titularidad pública como son las relativas a su creación, modificación o supresión (art. 20) y a la comunicación de datos entre Administraciones Públicas (art. 21). También contiene la LOPD disposiciones referidas a los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado (art. 22) y regula determinadas excepciones o restricciones de los derechos de los ciudadanos (derechos de acceso, rectificación y cancelación) con relación a los ficheros de datos policiales o de la Hacienda Pública (arts. 23 y 24)

[34] Es relativamente frecuente, por ejemplo, la imposición de sanciones a Ayuntamientos que realizan o toleran vertidos no autorizados, con el consiguiente quebranto para el dominio público hidráulico.

prudencia del legislador para que la implantación de la nueva normativa no resulte excesivamente perturbadora; pero también puede verse en la inusual duración de aquel periodo de carencia un indicio de falta de determinación a la ahora de asumir la efectiva implantación de aquellos principios y pautas de actuación que la LOPD proclama con el mayor énfasis.

III. Resulta necesario mencionar también otro factor cuya toma en consideración es inexcusable a la hora de calibrar las posibles inercias y resistencias que dificultan la efectiva aplicación de los mecanismos legales previstos para una protección efectiva de los datos de carácter personal. Me refiero al formidable volumen de negocio real o potencial que subyace —a veces no se conoce pero se intuye— en la creación, el tratamiento, el uso y la cesión de toda clase de ficheros y bases de datos personales.

Si la información es poder —y en este caso el tópico es enteramente certero—, no cabe duda de que su valor se incrementa enormemente si aquélla se presenta y ofrece en el mercado debidamente sistematizada, clasificada y con toda clase de posibilidades de acceso, criterios de búsqueda y selección, etc. El vertiginoso avance de la ingeniería informática y de las técnicas de almacenamiento y tratamiento de la información ofrece hoy día posibilidades que eran inimaginables hace unos años; y ello ha propiciado el nacimiento y desarrollo no menos vertiginoso de toda una industria tan dinámica y agresiva desde el punto de vista empresarial como reacia a que sus iniciativas y potencialidades se vean constreñidas por enojosos controles y trabas intervencionistas.

Es fácil imaginar, aunque las cifras son en realidad inimaginables, el volumen de negocio que se mueve en torno a los ficheros de datos, listados de clientes, bases de datos selectivas referidas a segmentos de población clasificados por edad, profesión, poder adquisitivo... o cualesquiera otros criterios que definan el perfil de potenciales clientes y usuarios. Ello por no mencionar los archivos de solvencia patrimonial y ficheros de morosos, que, al margen de movilizar un importante negocio basado en el valor intrínsico de la información que gestionan, ejercen una influencia determinante en las operaciones comerciales, financieras y crediticias de las personas o entidades titulares de los datos que allí se contienen. Pues bien, dejando sentado que muchas de las empresas dedicadas a las actividades mencionadas cumplen de manera satisfactoria los requerimientos de la normativa sobre protección de datos personales, es lo cierto que otras muchas —sobre todo empresas medianas y pequeñas cuya existencia es a veces efímera— operan al margen de aquellos controles. Y el fenómeno es grave porque no se trata ya de que incurran en acciones infractoras más o menos aisladas, sino que toda la actividad de la empresa está instalada en la ilegalidad, por ser éste precisamente el presupuesto de su existencia o, al menos, de su abultado margen de beneficio. Sucede que hacerse con una base de datos de clientes, de usuarios, de profesionales, etc., para luego comerciar con ella en el mercado es cosa bien asequible a condición de que no se tenga el escrúpulo de querer saber la proce-

dencia de los datos ni se pretenda constatar que se ha recabado el consentimiento de los afectados. En cambio, la confección de esa misma base de datos es mucho más dificultosa —y su explotación, por tanto, menos rentable— si ha sido elaborada con las debidas garantías y con plena observancia de los requerimientos de información y consentimiento de los afectados que exige la legislación sobre protección de datos personales.

Igual que ocurre con la reproducción ilegal de grabaciones musicales y de películas en formato *dvd*, el hecho de que la infracción sea tan asequible y el margen de rentabilidad tan grande son factores que determinan que el mercadeo de los ficheros de datos de carácter personal se produzca, con demasiada frecuencia, al margen de la legalidad. Además, el riesgo de sanción no es tan disuasorio como debiera pues ya hemos visto que la escasa concienciación ciudadana sobre la necesidad de protección de este derecho fundamental hace que no abunden las denuncias; y, por otra parte, la cuantía de las multas, con no ser desdeñable, no garantiza que vaya a quedar enteramente neutralizado el beneficio ilegalmente obtenido[35].

IV. Para finalizar este rápido recorrido cabe concluir que, aun reconociendo que desde la promulgación de la LORTAD de 1992 y luego con la LOPD de 1999 se han obtenido logros significativos, estamos aún lejos de alcanzar un nivel razonable de efectividad en la protección de los datos de carácter personal. Y para que tal cosa suceda será necesario, antes que una nueva reforma legal, la decidida utilización por parte de la Agencia de Protección de Datos de todos los instrumentos y vías de actuación que el legislador ha puesto en su mano; una mayor sensibilización de las Administraciones Públicas en cuanto a la necesidad de registrar sus ficheros de datos y de ser respetuosos con la normativa sobre medidas de seguridad y garantías en los procedimientos de recogida, tratamiento y cesión de tales datos; y, en fin, una paulatina concienciación de los ciudadanos sobre la relevancia del derecho a la protección de sus datos personales y sobre la importancia de ser beligerantes en la reivindicación y defensa de este derecho fundamental.

[35] Aunque el importe de los beneficios obtenidos por el infractor es uno de los criterios previstos en la norma para la graduación de las sanciones en materia de protección de datos personales (art. 45.4 LOPD), lo cierto es que las multas tienen en todo caso un tope cuantitativo máximo (apartados 1, 2 y 3 del propio art. 45), por lo que en caso de beneficios abultados la infracción puede resultar rentable a pesar de la sanción. Esto nos lleva a evocar la prevención establecida en otros ámbitos de la acción administrativa sancionadora, por ejemplo la legislación urbanística, donde la constatación de que el beneficio derivado de la conducta infractora es superior a la cuantía de la sanción permite incrementar el importe de la multa hasta hacerlo equivalente al beneficio ilícito (art. 231 del Texto Refundido de la Ley del Suelo, aprobado por Real Decreto 1346/1976, de 9 de abril).