DERECHO ADMINISTRATIVO

Seguridad del Estado y privacidad

Ofelia Tejerina Rodríguez

Doctora en Derecho. Abogada

Prólogo de

José Luis Piñar Mañas

Catedrático de Derecho Administrativo
Exdirector de la Agencia Española
de Protección de Datos

COLECCIÓN DE DERECHO ADMINISTRATIVO

TÍTULOS PUBLICADOS

El derecho de acceso a archivos y registros administrativos, *Leonor Rams Ramos* (2008).

Nuevo marco jurídico del sector ferroviario. Estudio de la Ley del Sector Ferroviario y demás normas de desarrollo, *Juan García Pérez* (2010).

La Contratación del Sector Público tras las reformas de 2010, *Álvaro Canales Gil y Justo Alberto Huerta Barajas* (2010).

La Administración instrumental en el proceso, *Alejandra Boto Álvarez* (2011).

La política de la Unión Europea en materia de turismo y sus repercusiones en la legislación turística española, *Antonio Villanueva Cuevas* (2012).

La terminación anormal del proceso contencioso-administrativo, *Luis Mª Bremond Trian*a (2013).

El régimen de contratación de los poderes adjudicadores que no son Administración pública, *Marta Oller Rubert* (2013).

Crisis económica y crisis del estado de bienestar. El papel del Derecho Administrativo, *José Luis Piñar Mañas (Coord.)* (2013).

Seguridad del Estado y privacidad, *Ofelia Tejerina Rodríguez* (2014).

COLECCIÓN DE DERECHO ADMINISTRATIVO

Director
JOSÉ LUIS PIÑAR MAÑAS
Catedrático de Derecho administrativo

SEGURIDAD DEL ESTADO Y PRIVACIDAD

Ofelia Tejerina Rodríguez
Doctora en Derecho. Abogada

Prólogo de
José Luis Piñar Mañas
Catedrático de Derecho Administrativo
Exdirector de la Agencia Española de Protección de Datos

Madrid, 2014

DERECHO ADMINISTRATIVO

C/ Rafael Calvo, 18, 2º C – 28010 Madrid
Tfno.: (34) 91 521 36 19 – (34) 91 522 30 54
Fax: (34) 91 445 11 26
E-mail: reus@editorialreus.es
http://www.editorialreus.es

1.ª edición REUS, S.A. (2014)
ISBN: 978-84-290-1769-4
Depósito Legal: M 13987-2014
Diseño de portada: María Lapor
Impreso en España
Printed in Spain

Imprime: Talleres Editoriales Cometa, S. A.
Ctra. Castellón, km 3,400 – 50013 Zaragoza

ÍNDICE

PRÓLOGO 9

INTRODUCCIÓN 15

I. EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 19

1. Contenido y alcance 19

1.1. Origen del derecho: la protección de la libertad 19

1.2. Contenido: la información personal 22

1.3. El bien jurídicamente protegido: el derecho a decidir 29

1.4. Concepto práctico de la «Protección de datos» 34

2. Reconocimiento normativo 39

2.1. El artículo 18 en la CE; desarrollo normativo y jurisprudencial 39

2.2. Legislación y contribución jurisprudencial de la Unión Europea y Estados miembros 72

3. Las garantías: «El ciudadano de cristal» 95

3.1. Transparencia y ejercicio de derechos 95

3.2. Medidas de seguridad; regulación 106

3.3. Tecnologías para la Protección (PET) 117

3.4. Identificador único 121

II. CONTROL ESTATAL DEL CIUDADANO 127

1. Intervención de las autoridades; seguridad ciudadana y estados excepcionales 127

2. Fuerzas y Cuerpos de Seguridad del Estado; ficheros de datos 141

2.1. El tratamiento de datos al servicio de la Policía 143

2.2. Ficheros Policiales; tipología. 157

2.3. Seguridad de los Datos 161

2.4. Criterios de la AEPD 173

III. TECNOLOGÍAS DE CONTROL ESTATAL 179

1. Control de las comunicaciones electrónicas 179

1.1. Secreto de las comunicaciones 182

1.1.a. El concepto del secreto 182
1.1.b. La Directiva sobre la privacidad y las comunicaciones, y su reflejo en el derecho interno español 192
1.1.c. Jurisprudencia 202
1.1.d. Vulneración del secreto por agentes públicos 209
1.1.e. Intervención del ordenador personal 216
1.2. Retención de datos 226
1.2.a. Antecedentes 226
1.2.b. La Directiva y su trasposición en España 234
1.2.c. Reticencias en Europa y nulidad de la Directiva 241
1.3. Interceptación de las comunicaciones 248
1.3.a. Cobertura legal 248
1.3.b. Respaldo de los tribunales 260
2. Videovigilancia 283
2.1. Normativa española para el Sector Público 292
2.2. Normativa en la UE 303
3. Bases de datos genéticas 312
3.1. Posibilidades de tratamiento para las autoridades policiales 314
3.2. Regulación normativa y criterios de la AEPD 319
3.3. Europa: Grupo de Trabajo del Artículo 29 y Tratado de Prum .. 326
3.4. La Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN 330
4. «Passenger Name Record» (PNR) 333
5. Escáneres de protección en aeropuertos 349
6. El Código «SWIFT».... 355

V. CONCLUSIONES: ESTADO DE DERECHO, SEGURIDAD Y PROTECCIÓN DE DATOS 359

BIBLIOGRAFÍA 367

PRÓLOGO

Pocos libros pueden ser más oportunos en este momento como el de Ofelia Tejerina sobre Seguridad del Estado y Privacidad[1].

Elaborado bajo la dirección del Prof. Ignacio TORRES MURO y yo mismo para la obtención del grado de Doctor en Derecho, es fruto del tesón, la dedicación y el esfuerzo de la autora, que ya contaba, desde antes de iniciar su Tesis, con un importante bagaje de conocimientos en torno a un tema que hoy se presenta como uno de los más centrales en la construcción de la democracia.

Como ha señalado Wolfang SOFSKY, «la privacidad es la ciudadela de la libertad personal»[2] y sin embargo, como se ha puesto de manifiesto hasta la saciedad, hoy está en peligro como nunca antes lo había estado. Nada nuevo decimos cuando afirmamos tal cosa, pero no debemos por ello pensar que ningún remedio es posible para evitarlo. En alguna ocasión también me he referido a ello[3] y he reivindicado que cuanto más riesgos corre la privacidad más empeño hemos de poner en evitar que se alcance una situación que puede llegar a ser irreversible. Una realidad en la que sea posible que sepan todo de nosotros[4].

Pero lo realmente peligroso no es ya que puedan saber todo de nosotros, ni siquiera que lo que sepan de cada una de las personas se utilice para bombardearnos con una constante e indeseada publicidad, sino que esa situación condicione, dirija nuestras vidas. El panópticon de Jermy BENTHAM[5], cuya

---

[1] Libro que se ha llevado a cabo en parte en el marco del Proyecto de Investigación sobre «Protección de Datos y aplicación extraterritorial de las normas», Ref. DER 2012-35948, del Programa I+D del Ministerio de Economía y Competitividad, del que soy Investigador Principal.

[2] *Defensa de lo privado*, Pre-Textos, Valencia, 2009, p. 53.

[3] Por ejemplo, en *¿Existe la privacidad?*, Ediciones CEU, Madrid, 2008, también recogido en *Protección de datos Personales. Compendio de lecturas*, edición de la Cámara de Diputados y el IFAI, México, 2010, pp. 15 y ss.

[4] Véase Stephen BAKER, *Numerati. Lo saben todo de ti*, Seix Barral, Barcelona, 2009.

[5] Redactado en 1791 como Memoria que entregó a través de Jean Philippe GARRAN DE COULON a la Asamblea Nacional para una posible reforma de las leyes penales en Francia.

cita es lugar común al hablar de privacidad, se considera superado y se habla ahora también de «banopticon», para hacer referencia, por un lado, al hecho de que los vigilados colaboran con los vigilantes y facilitan su propia vigilancia, pero sobre todo, por otro, a que la tecnología de la vigilancia actual permite la exclusión de colectivos ingentes de personas[6].

La privacidad amenazada, además, se vuelve mucho más vulnerable cuando frente a los avances y retos de las nuevas tecnologías, que se mueven en un ámbito sustancialmente ajeno a la idea de territorio, se pretende reaccionar con marcos normativos tradicionales apegados al territorio. Sin olvidar que en no pocas ocasiones son las propias normas las que ponen en situación de riesgo a la privacidad. Como ha señalado Stefano RODOTÀ, estamos en riesgo de perder «no sólo… toda intimidad, sino también… la posesión del yo, expropiado por quienes tienen la posibilidad de observarnos y reconstruir a su antojo toda nuestra identidad, la totalidad de nuestro cuerpo electrónico», y en este escenario «la dimensión supranacional y las políticas de seguridad podrían anular las garantías existentes». Es por ello necesario contar con instrumentos internacionales que superen esa idea de extraterritorialidad e impidan la aparición y consolidación de «paraísos informáticos»; así como la propia amenaza que suponen algunos marcos normativos que, como los surgidos tras los atentados del 11 de septiembre de 2001 en Nueva York, permiten (tal es el caso de la *Patriot Act*) a una serie de sujetos públicos el pleno acceso a cualquier base de datos, público o privado, restringiendo y aún eliminando las garantías que deberían reconocerse en relación con el respeto a la protección de datos[7].

Cobra entonces especial interés la búsqueda del necesario equilibrio entre seguridad pública y privacidad. Y ese es el objetivo esencial del libro de Ofelia Tejerina. Libro que acierta a exponer el grueso de las cuestiones que en la actualidad giran en torno a esa relación nada fácil entre seguridad y protección de datos.

Y que, como señalaba al principio, debe leerse ahora con mayor motivo tras haberse publicado la capital Sentencia del Tribunal de Justicia de la Unión

---

Sobre el Panopticon de BENTHAM la bibliografía es inabarcable. Recientemente vid. Anne Brunon-Ernst (Ed.) *Beyond Foucault: New Perspectives on Bentham's Panopticon*, Ashgate Publishing, 2013.

[6] Sobre la idea de «banopticon» vid. Didier BIGO, «Globalized (in) security: the field and the banopticon», en Naoki SAKAI y Jon SOLOMON (Eds.) Revista *Traces,* Vol. 4, sobre *Translation, Biopolitics, Colonial Difference*, Hong Kong University Press, 2006. Asimismo, Zygmunt BAUMAN y David LYON, *Vigilancia líquida*, Paidos, Barcelona, 2013, pp. 61 y ss.

[7] *La vida y las reglas. Entre el derecho y el no derecho*, Trotta, Madrid, 2010, p. 102 (con Prólogo de José Luis Piñar Mañas).

Europea de 8 de abril de 2014[8], asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger y otros* por la que se declara la invalidez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, conocida como Directiva sobre retención de datos.

La Directiva, que desde su origen fue enormemente polémica y que ya había sido traspuesta por los Estados miembros, regulaba la obligación de retención de numerosos datos de tráfico de millones de personas. No es, o era, la única norma sobre retención de datos, pues también en Estados Unidos se cuenta con normas que la regulan[9], pero sí se ha considerado particularmente invasiva de la protección de datos. Y ello en el marco de las relaciones entre seguridad pública y privacidad. Tan polémica es la regulación de la retención de datos que, como cumplidamente señala Ofelia Tejerina en el libro, el Tribunal Constitucional rumano (octubre de 2009), el Tribunal Constitucional Federal alemán (marzo de 2010) y, el Tribunal Constitucional checo (marzo de 2011) han anulado sus respectivas leyes de transposición de la Directiva por considerarlas inconstitucionales.

La Sentencia analiza la Directiva 2006/24/CE confrontándola con los artículos 7 y 8 de la Carta Europea de Derechos Humanos (no llega a analizar el impacto del artículo 11, sobre libertad de expresión y de información). El primero reconoce el derecho a la vida privada y familiar; el segundo el derecho a la protección de datos de carácter personal. El Tribunal parte de la base de que los datos a los que se refiere el artículo 5 de la Directiva (los datos que deben ser retenidos, que por cierto son muy dispares y numerosos) tomados como un todo, pueden permitir obtener muy precisas conclusiones referentes a las vidas privadas de las personas cuyos datos son retenidos, tales como sus hábitos diarios, lugares permanentes o temporales de residencia, movimientos diarios o de otro tipo, actividades desarrolladas, relaciones sociales y ambientes sociales que frecuentan (apartado 27). La retención de tales datos, con el fin de su posible acceso por parte de las autoridades nacionales competentes, afecta «directa y específicamente a la vida privada» y por tanto a los derechos reconocidos por el artículo 7 de la Carta; además, dado que dicha retención implica un tratamiento de datos, es de aplicación

[8] Es decir, cuando hacía tiempo que el libro estaba concluido, e incluso cerrada la corrección de pruebas en la Editorial.

[9] Sobre los modelos americano y europeo de retención de datos es interesante el trabajo de Miguel RECIO, *Data Retention: A Comparative Analysis of the ECPA and thee Privacy Directive*, Georgetown UniversityLaw Center, Washington, 2008 (ejemplar que amablemente me ha facilitado el autor).

el artículo 8 y por tanto es necesario respetar las exigencias que se deducen de tal precepto (apartado 29 de la Sentencia).

Dicho lo anterior, el Tribunal, tras recordar que es indiferente que los datos retenidos sean o no sensibles, afirma que la retención de datos, tal como está regulada en la Directiva 2006/24, constituye en sí misma una interferencia respecto de los derechos garantizados por los artículos 7 y 8 de la Carta. Y advierte no sólo que tal interferencia es «particularmente seria», sino que el hecho de que los datos sean retenidos y posteriormente usados sin que los abonados o usuarios sean informados de ello puede generar en los mismos «la idea de que sus vidas privadas están sujetas a una constante vigilancia» (apartado 37). Lo que exige analizar si la interferencia de los derechos reconocidos en los reiterados artículos 7 y 8 está justificada.

Para ello recuerda que el artículo 52.1 de la Carta dispone que «Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás». Partiendo de ello, en lo que se refiere al interés general, y en lo que afecta en particular a la seguridad pública, destaca que la lucha contra el terrorismo para mantener la paz y la seguridad constituye un objetivo de interés general, sin olvidar, además, que el propio artículo 6 de la Carta reconoce el derecho de toda persona a la seguridad (apartados 41 a 44 de la Sentencia). Ahora bien, siendo esto así, es imprescindible determinar si las medidas adoptadas en la Directiva respetan o no el principio de proporcionalidad. A tal fin, el Tribunal parte de la base de que, al interferir la Directiva con derechos fundamentales, la discrecionalidad del legislador comunitario «es reducida, con el resultado de que el control sobre la misma debe ser estricto» (apartado 48). En este sentido, el Tribunal analiza si las medidas previstas en la Directiva son apropiadas y necesarias. En cuanto al primer criterio, el Tribunal admite que la retención de datos puede ser una medida apropiada para la investigación criminal. Admite incluso que la lucha contra los delitos graves, en particular contra el crimen organizado y el terrorismo, es de gran importancia para garantizar la seguridad pública, pero, en cualquier caso tal objetivo de interés general, por muy fundamental que pueda ser, no justifica en sí mismo que las medidas de retención tal como están previstas en la Directiva 2006/24 sean consideradas necesarias para la finalidad de tal lucha (apartado 51). Entre otros aspectos, el Tribunal resalta que la Directiva, al alcanzar a tal número y naturaleza de datos, implicar a todas las formas de comunicaciones electrónicas y afectar a todos los abonados y usuarios, implica «una interferencia en los derechos fundamentales de la práctica totali-

dad de la población europea» (apartado 56). Asimismo critica que la Directiva afecta a todas las personas, incluidas aquellas sometidas a la obligación del secreto profesional; no contiene criterios objetivos en cuanto a los límites en el acceso a los datos por parte de las autoridades nacionales competentes; contiene una referencia a «delitos graves» que es muy genérica; carece de condiciones sustantivas y procedimentales relativas al acceso y subsiguiente uso de los datos; no limita las autoridades que pueden tener tal acceso; no incluye criterio objetivo alguno para determinar el límite temporal que debe entenderse estrictamente necesario en relación con la retención de los datos, que puede ir desde 6 meses a 2 años. Todo lo anterior lleva al Tribunal a la conclusión de que la Directiva supone una particularmente seria interferencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta sin que pueda precisarse si la misma es estrictamente necesaria. Además, la Directiva tampoco contiene previsiones precisas acerca de las medidas de seguridad de índole técnica y organizativa que deben adoptarse para asegurar la integridad y confidencialidad de los datos (apartados 57 a 67), ni exige que los datos retenidos permanezcan en la Unión Europea (apartado 68), lo que lleva al Tribunal a concluir que la Directiva no respeta el principio de proporcionalidad exigido por el artículo 52.1 de la Carta, en relación con los artículos 7 y 8, y por lo tanto debe ser declarada «inválida».

No es este lugar para profundizar más en una Sentencia cuyas consecuencias son difíciles de prever. En cualquier caso, creo que subrayar estos importantes y novedosos detalles, en el contexto del magnífico libro que el lector tiene en sus manos, era necesario pues, además, coincide en gran medida con las conclusiones que la autora alcanza tras una investigación, como decía al principio, seria, rigurosa y concienzuda. Quizá estemos ante un síntoma de que el Derecho puede generar todavía esperanzas en la lucha por la privacidad y la protección de datos.

En definitiva se trata de resaltar, como lo hace Ofelia Tejerina, que en la tensión entre seguridad pública —o seguridad del Estado— y privacidad, no debemos nunca olvidar los principios que el legislador debe respetar cuando setrata de limitar un derecho fundamental. Pues no es que esté en juego «sólo» el derecho a la protección de datos; es que está en juego el entero sistema democrático. Y por ello aportaciones como la que ahora nos ofrece Ofelia Tejerina no pueden más que ser muy bien venidas.

Madrid, 27 de abril de 2014

JOSÉ LUIS PIÑAR MAÑAS
Catedrático de Derecho Administrativo.
Ex Director de la Agencia Española de Protección de Datos