

Régimen jurídico aplicable a la protección de datos de carácter personal

Conchita Urda Serrano

(IberForo-Madrid)

I. INTRODUCCIÓN

La protección de los datos de carácter personal está adquiriendo en los últimos tiempos una gran relevancia: cada día el ciudadano es más consciente de los derechos que le asisten en relación a sus propios datos; desde las instancias públicas se presta más atención al tema y las empresas muestran una mayor sensibilidad al respecto. En ello ha influido mucho la actividad creciente de la Agencia de Protección de Datos, organismo autónomo encargado de asegurar el cumplimiento de la legislación vigente. Así, en 1999, la Agencia aumentó de forma espectacular su actividad e incluso dobló la cantidad impuesta en multas el año anterior, superando los 1.500 millones de pesetas.

Por todo ello, es conveniente conocer la normativa española aplicable a este tema, modificada recientemente y puesta en práctica de manera mucho más estricta que la antigua LORTAD de 1992. Seguidamente, haremos una breve referencia a los aspectos más importantes y novedosos de la legislación vigente.

II. NORMATIVA VIGENTE

El marco normativo en que se encuadra la materia de protección de datos de carácter personal es el siguiente:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD).
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal.
- Real Decreto 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la Ley Orgánica 5/1992 (antigua LORTAD¹).

Asimismo, existen varias instrucciones de la Agencia de Protección de Datos en relación a temas específicos, como la notificación y el registro de ficheros de datos personales², los derechos de acceso, rectificación y cancelación en ficheros automatizados³ o la transferencia internacional de datos⁴, entre otras.

III. LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

La legislación española de protección de datos de carácter personal es, desde la promulgación de la nueva LOPD, muy garantista de los derechos de la persona que

comunica sus datos personales, sin olvidar que la ley sólo contempla bajo su ámbito de aplicación los datos de personas físicas, no jurídicas.

La LOPD entró en vigor en enero del año 2000, y se caracteriza por ser más estricta y rigurosa que la ley anterior (la LORTAD de 1992), contemplando la posibilidad de imponer multas elevadas en caso de infracción por incumplimiento de las obligaciones establecidas en la ley. Siempre que se lleve a cabo un tratamiento de datos personales, es decir, siempre que se realice cualquier operación o procedimiento técnico que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo y/o cancelación de cualquier tipo de información concerniente a personas físicas identificadas o identificables, resulta aplicable la LOPD y su normativa de desarrollo. Por lo tanto, toda persona que obtenga y/o mantenga en su poder datos personales de particulares está obligada al cumplimiento de ciertas obligaciones.

Responsable y encargado del tratamiento de datos personales

Sin embargo, la ley diferencia entre dos figuras que pueden quedar sujetas a estas obligaciones: el responsable del tratamiento y el encargado del tratamiento.

El responsable es la persona física o jurídica que va a decidir sobre la finalidad, contenido y uso del tratamiento de los datos personales. Los ficheros de datos personales pueden ser de titularidad pública o privada, dependiendo del responsable del tratamiento. Si se trata de una Administración Pública, el fichero será público y deberá regirse por las reglas específicas al respecto contenidas en la LOPD. En el caso de ficheros privados, sus responsables se hallan sujetos a numerosas obligaciones respecto a la protección de los datos, como por ejemplo la obligación de notificar a la Agencia de Protección de Datos acerca de la existencia del fichero, su contenido y su finalidad, y la inscripción correspondiente del fichero en el Registro General de Protección de Datos; la obligación de proporcionar determinada información a los titulares de los datos y la obtención de su consentimiento para el tratamiento de los datos.

Por su parte, el encargado del tratamiento, figura nueva introducida por la ley, es un tercero que accede a los datos cuando dicho acceso es necesario para la prestación de un servicio al responsable del tratamiento. Por ejemplo, es el caso de una empresa que contrata a otra para que realice una campaña de marketing con los datos de sus clientes. Se establece una relación contractual (un arrendamiento de servicios) entre el responsable del tratamiento y este tercero, debiendo estar regulada dicha relación por un contrato escrito, o de otra forma que permita acreditar su celebración y contenido, en el que debe constar que (i) el encargado del tratamiento tratará los datos conforme a las instrucciones del responsable del tratamiento; (ii) no los utilizará con fines distintos a los que figuren en el contrato; (iii) no los comunicará, ni siquiera para su conservación, a otras personas; (iv) implementará las medidas de seguridad que le correspondan. Asimismo, el encargado deberá devolver o distribuir los datos a su propietario, una vez concluida la prestación contractual, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

¹ Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

² Resolución de 30 de mayo de 2000, de la Agencia de Protección de Datos, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático a través de los que deberán efectuarse las solicitudes de inscripción en el Registro General de Protección de Datos. (BOE 27/06/2000).

³ Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación en ficheros automatizados (BOE 29/1/1998).

⁴ Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos (BOE 16/12/2000).

Derechos de los titulares de los datos personales

Además de la importante distinción entre la figura de responsable y la de encargado, la ley otorga diversos derechos al "afectado" o "interesado", denominación por la que se designa a la persona física titular de los datos que sean objeto del tratamiento. Son los derechos de acceso, cancelación, oposición y rectificación.

Estos derechos pueden ser ejercidos únicamente por el interesado o, en su caso por un representante legal, frente al responsable del tratamiento el cual está obligado a responder al interesado; en caso contrario incurrirá en una infracción. Además, el responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

Otras características de la LOPD

Otras características importantes de la LOPD son las siguientes:

- La LOPD es aplicable a todo tratamiento de datos personales, sea automatizado o no.
- En relación al concepto de "cesión de datos", la LOPD no resulta muy esclarecedora puesto que se limita a identificar "cesión" y "comunicación" de datos, y las define como "*toda revelación de datos realizada a una persona distinta del destinatario.*" La regla general es que toda cesión de datos requiere consentimiento del interesado, salvo previsión legal expresa. El incumplimiento de esta obligación está tipificado como infracción muy grave, lo cual conlleva una sanción que oscila entre 50 y 100 millones de ptas.
- La LOPD establece de forma taxativa las fuentes de acceso público para obtener información, considerando como tales el censo promocional (censo elaborado por el Instituto Nacional de Estadística a partir de los datos del censo electoral), los repertorios telefónicos, las listas de personas pertenecientes a grupos de profesionales, diarios y boletines oficiales y medios de comunicación. Si los datos personales proceden de tales fuentes, entonces no es necesario el consentimiento de los titulares de los datos pero sí será necesario comunicarles, en un plazo máximo de 3 meses desde el registro de los datos, la existencia, contenido y finalidad de dicho tratamiento de datos así como la identidad del responsable del mismo.
- La Agencia de Protección de Datos es la encargada de supervisar el cumplimiento de la LOPD, y para ello, actúa tanto de oficio como a raíz de las denuncias presentadas. La Agencia puede imponer multas que oscilan entre las 100.000 ptas y los 100.000.000 ptas, dependiendo de la infracción cometida (leve, grave o muy grave). Estas cantidades son mucho más altas que las previstas en el resto de la Unión Europea.

IV. MEDIDAS DE SEGURIDAD

Las medidas de seguridad aplicables dependen del tipo de información a la que se refieran los datos personales. La LOPD otorga una especial protección a determinados datos como los relativos a ideología, religión o creencia, origen racial, salud y vida sexual, incluyendo como novedad los datos sobre afiliación sindical. En este sentido, el RD 994/1999, relativo a medidas de seguridad, distingue entre:

- Datos de nivel básico: son los datos de carácter personal. El plazo para implantar las medidas de seguridad en relación a estos datos acabó el 26 de marzo de 2000⁵.
- Datos de nivel medio: son los datos relativos a la comisión de infracciones administrativas o penales, servicios financieros y aquellos que permitan evaluar la personalidad del individuo. Esto último se refiere a datos que separadamente se incluirían en el nivel básico, pero que tomados en conjunto conforman un perfil de la persona (características personales, circunstancias sociales, datos académicos y profesionales, empleo, información económico-financiera, etc.). Las medidas de nivel medio debían ser implantadas antes del 26 de junio del 2000⁶.
- Datos de nivel alto: son los datos de ideología, religión, creencias, origen racial, salud, vida sexual o datos recogidos con fines policiales. El plazo para implantar estas medidas ha sido recientemente ampliado hasta el 26 de junio de 2002⁷.

Dependiendo del tipo de datos, las medidas de seguridad que debe adoptar el responsable del fichero para garantizar la confidencialidad y seguridad de los datos serán diferentes. En todo caso, las medidas que correspondan deberán ser implantadas sin necesidad de notificar dicha implantación a la Agencia de Protección de Datos.

Así, en el caso de datos de nivel básico, el responsable del fichero deberá plasmar la normativa de seguridad de la empresa en el denominado "documento de seguridad", el cual contendrá información sobre los recursos protegidos, las medidas de seguridad tomadas, las funciones y obligaciones del personal, la estructura de los ficheros y descripción de los sistemas de información que los tratan, el procedimiento de notificación, gestión y respuesta ante las incidencias y los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Para los datos de nivel medio, además de este documento de seguridad, se requiere el sometimiento a una auditoría informática al menos cada dos años, la identificación y autenticación de las personas con acceso autorizado a los datos, un control de acceso físico y un sistema de control de soportes.

⁵ Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento.

⁶ Cit. Supra.

⁷ Resolución de 22 de junio de 2001, de la Subsecretaría, por la que se dispone la publicación del Acuerdo de Consejo de Ministros por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información.

Por último, para los datos de nivel alto, se exigen además medidas de seguridad para la distribución de soportes, un registro de accesos, conservación de copias de respaldo en un lugar diferente de aquel en que se encuentren los equipos informáticos que tratan los datos y cifrado de los datos cuando éstos se transmitan a través de redes de telecomunicación.