



Cristina Almuzara Almaida

ABOGADO. ESPECIALISTA EN PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

La protección de datos personales en España se encuentra regulada en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por la que se transpone a la legislación española los principios y disposiciones establecidos en la Directiva 45/95/CE, de 24 de octubre, del Parlamento Europeo y del Consejo, 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.

El ámbito de aplicación de la Ley Orgánica 15/1999 (en adelante, LOPD) se centra en la protección de las personas físicas, dado el marco regulador de la Ley previsto tanto en la citada Directiva como en el artículo 18.4 de nuestra Constitución, el cual dispone que deberá limitarse el uso de la informática para evitar posibles abusos en el honor y la intimidad personal y familiar de los ciudadanos. Por tanto, no se encuentran amparadas bajo esta normativa a las personas jurídicas, si bien la abundante jurisprudencia del Tribunal Supremo ha reconocido la existencia del derecho al honor de las personas jurídicas.

La LOPD, al igual que su predecesora –la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de Datos de Carácter Personal (LORTAD)– sienta su regulación sobre dos pilares fundamentales: el principio del consentimiento y el principio de finalidad. Estos principios implican que todo tratamiento de datos personales requiere el consentimiento inequívoco del interesado, si bien la LOPD establece un régimen de excepciones a la necesidad del consentimiento; por su parte, el principio de finalidad requiere que el interesado deberá conocer el alcance específico y concreto del uso de sus datos personales por parte del responsable del tratamiento.

La Sentencia del Tribunal Constitucional 292/2000, de 30 noviembre, ha delimitado el concepto y alcance del derecho fundamental de la pro-

Introducción y principios de la Ley Orgánica 15/1999, reguladora de la protección de datos de carácter personal



tección de datos personales. A este respecto el Tribunal indica que el objeto de este derecho fundamental es «garantizar a esa persona un poder

de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del



afectado». Por su parte, esta Sentencia configura el derecho a la protección de datos como un derecho fundamental autónomo e independiente del derecho a la intimidad personal y familiar, definido como «un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos puede proporcionar a un tercero, sea el Estado o un particular, o cuáles puede recabar este tercero, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión y usos».

Los principios en los que se asientan las bases de la LOPD se enuncian en el Título II de la Ley (artículos 4 al 12), de los que se derivan una serie de derechos para las personas afectadas, que son desarrollados en el Título III.

Centrando el análisis de los principios de la Ley, y como se ha indicado anteriormente, el consentimiento supone las premisas en las que se asientan la regulación de la LOPD, requiriéndose así su otorgamiento inequívoco por parte del interesado, tanto para el tratamiento como para la cesión o comunicación a terceros de sus datos por el responsable del fichero. Este principio general tiene ciertas excepciones basadas fundamentalmente en la existencia de habilitación legal para su tratamiento y/o cesión; en la necesidad de su tratamiento para el mantenimiento y cumplimiento de las relaciones negociales, contractuales, laborales o administrativas (y así entre las excepciones al consentimiento para la cesión de datos se citan, entre otros al Defensor del Pueblo, Tribunal de Cuentas o instituciones autonómicas con funciones análogas a éstos); en la prevención para el diagnóstico médico, prestación de asistencia o urgencia sanitaria; en la cesión al Ministerio Fiscal, Jueces o Tribunales, o cuando procedan de fuentes accesibles al público.

La regla general del consentimiento inequívoco se encuentra reforzada cuando se tratan datos especialmente protegidos (regulados en el artículo 7

de la LOPD) y para los cuales se exige el consentimiento expreso cuando los datos hagan referencia al origen racial, a la salud y a la vida sexual; y el consentimiento expreso y por escrito para proceder al tratamiento de datos que revelen ideología, afiliación sindical, religión o creencias.

No obstante, el artículo 12 de la LOPD, si bien no regula ninguna excepción a la cesión de datos personales, sí precisa que no se considerará comunicación de datos el acceso de un tercero (definido en la Ley como encargado del tratamiento) cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. En

Los datos tratados por parte del responsable del fichero deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se hayan obtenido

estos casos, será necesario regular en un contrato de prestación de servicios los requisitos mencionados en el citado artículo para que dicho acceso no se considere cesión de datos a los efectos de la Ley.

Pero con independencia de la necesidad o no del otorgamiento del consentimiento por parte de su titular, en todo caso deberá informarse al interesado de los requisitos señalados en el artículo 5 de la LOPD respecto del cumplimiento del derecho de información. Este principio resulta ineludible por parte del responsable del tratamiento y su importancia ha sido destacada en la Sentencia del Tribunal Constitucional a la que se ha aludido con anterioridad.

Por su parte, las normas de cali-

dad indican que los datos tratados por parte del responsable del fichero deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas, y legítimas para las que se hayan obtenido; que dichos datos sólo pueden usarse para finalidades compatibles con aquéllas para las que fueron recogidos (de esta forma, la finalidad que se consiente por el interesado, debe ser respetada por el responsable del tratamiento); que los datos deberán ser exactos y puestos al día, respondiendo con veracidad a la situación actual del afectado, por tanto, es deber del responsable del fichero cancelar o rectificar de oficio los datos registrados que no son exactos o que están incompletos, y que deben ser cancelados o sustituidos por los correctos. Y, por último, deberán cancelarse los datos (implicando el bloqueo de los mismos hasta que finalicen todas las posibles responsabilidades derivadas del tratamiento o de la legislación aplicable a los datos recabados) cuando los datos hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recogidos o registrados.

Los responsables de ficheros deberán establecer las medidas de seguridad necesarias para evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos bajo cuya responsabilidad se encuentran, incluido el deber de guardar secreto profesional respecto a los datos por parte del titular del fichero o las personas que intervengan en el tratamiento de datos por su cuenta. Estas medidas de seguridad se regulan en el Real Decreto 994/1999, de 26 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (que se encuentra en vigor, en virtud de la disposición transitoria tercera de la LOPD). ■