NUEVOS TIEMPOS PARA LA PROTECCIÓN DE DATOS PERSONALES Y SU REPERCUSIÓN EN LOS DESPACHOS DE ABOGADOS. BREVES NOTAS AL ESPERADO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

Ana Isabel Herrán Ortiz
Profesora Titular de Derecho civil.
Universidad de Deusto

Fecha de recepción: 12 de Junio de 2014
Fecha de aceptación: 24 Junio de 2014

RESUMEN: La evolución en el modelo de despacho profesional ha venido acompañada por la creciente incorporación de los avances tecnológicos en la labor de ejercicio profesional de la abogacía. Las innegables ventajas y bondades que estos avances representan, sin embargo, no pueden hacernos olvidar las indudables dudas e incertidumbres jurídicas que su utilización suscita. Por ello, la protección de datos personales constituye una necesidad legal a la que los despachos de abogados no pueden sustraerse. La inminente reforma de la normativa europea de datos personales nos ofrece una inmejorable oportunidad para reflexionar y analizar los principios, problemas y dificultades jurídicas que el tratamiento de datos personales encierra en el ejercicio de la abogacía.

ABSTRACT: The evolution in the professional model release has been accompanied by the increasing incorporation of technological advances in the work of the professional practice of law. The undeniable advantages and benefits that these developments represent can't obscure the undoubted legal doubts and uncertainties that use raises. Therefore, the protection of personal data is a legal necessity that law firms can't escape. The imminent reform of European legislation of personal data gives us an excellent opportunity to reflect and analyze the principles, problems and legal difficulties that the processing of personal data enclosed in the practice of law.

PALABRAS CLAVE: Protección de datos personales, despacho de abogados, computación en nube.

KEYWORDS: Protection of personal data, Law firm, cloud computing.

I. CUESTIONES PRELIMINARES

Puede afirmarse que en los últimos tiempos los despachos de abogados han vivido una significativa transformación en sus ámbitos de organización y gestión, de suerte que superando el tradicional modelo personalista se han constituido en auténticas empresas de servicios y asesoría legal. Esta evolución ha venido acompañada por el impulso en los despachos de abogados de las tecnologías de la información y la comunicación; y así, a las innegables ventajas de este fenómeno que todos acertamos a señalar, deben sumarse los posibles inconvenientes que esta incorporación presenta en el ejercicio de la abogacía. Uno de estos inconvenientes e incertidumbres que la implantación tecnológica implica para el ejercicio profesional es, sin duda, la necesaria tutela de la información personal, que todavía constituye en la actualidad una importante dificultad a la que se enfrentan día a día quienes ejercen su actividad profesional en un despacho de abogados. En efecto, desde el punto de vista de la normativa de protección de datos de carácter personal, lamentablemente, son numerosas las dificultades por vencer para la adaptación de los despachos de abogados a la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante LOPD), y a su Reglamento, aprobado mediante el Real Decreto 1720/2007, de 21 de diciembre, y en vigor desde el 19 de abril de 2008 (en adelante RLOPD)[1]. En futuro cercano, se impone además la aplicación de la nueva normativa europea de protección de datos personales, que en fechas no muy lejanas será una realidad a la que deberá hacerse frente también desde los diferentes Estados, empresas y particulares[2].

Sea como fuere, desde la perspectiva de la protección de datos personales, los responsables de un despacho de abogados, deben preguntarse si su despacho será capaz de reconocer y resolver posibles incidentes de seguridad que puedan alterar, destruir o ceder ilícitamente la información personal que en el ejercicio profesional es objeto de tratamiento. A este respecto, conviene recordar que la seguridad de la información en los despachos de abogados no representa una opción, o una alternativa, sino una necesidad y una exigencia legal que, como afirma Pérez Gómez, requiere en primer lugar, identificar riesgos y después, establecer los controles que eviten, minimicen o encaucen los posibles daños[3].

En este estudio, se pondrá de manifiesto que con arreglo al diferente modelo de organización y estructuración de los despachos de abogados, la tutela de la información personal y la garantía de su seguridad se enfrentan a diversas situaciones y conflictos jurídicos; de suerte que, en cada caso, deberá contemplarse la solución idónea para facilitar a los despachos de abogados su adaptación a la normativa de protección de datos personales. De igual modo, se tendrá ocasión de reflexionar a propósito de la próxima normativa europea sobre protección de datos personales y su incidencia en el ejercicio profesional de los abogados, analizando con especial atención las principales novedades jurídicas que su texto incorpora.

---

[1] RD 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/99, de 13 de diciembre, de protección de datos de carácter personal. BOE núm. 17, de 19 de enero de 2008, p. 4103-4136.

[2] Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). Doc. COM (2012) 11 final, de 25 de enero de 2012. En la actualidad, el parlamento ha adoptado recientemente enmiendas al citado texto; para información actual y completa véase Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).

[3] E. PÉREZ GÓMEZ, "¿Por qué proteger la información en los despachos de abogados?", *IURIS*, núm. 147, marzo de 2010.

II. DIMENSIÓN NORMATIVA DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN ESPAÑA

Con la proclamación constitucional del artículo 18.4 CE, por la cual "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", y hasta la entrada en vigor del RLOPD, la tutela de la información personal se ha enfrentado a un complejo, dilatado y agitado proceso, durante el cual desde los más diversos sectores se venía reclamando la aprobación de un desarrollo reglamentario específico para la LOPD, que ofreciera respuesta a cuantos problemas prácticos se planteaban en la tutela de los datos personales, y a los que la citada norma no otorgaba una satisfactoria solución.

Con todo, no fue sencillo ni pacífico el proceso seguido hasta la definitiva aprobación del actual Reglamento 1720/2007[4]; y si bien finalmente, la norma aprobada no cumplió con cuantas expectativas había despertado entre los expertos, lo cierto es que el RLOPD representó un importante avance en la configuración legal del derecho a la protección de datos personales en España. Ciertamente, dos son logros que con frecuencia destaca la doctrina de este texto legal, a saber: por una parte, se configura desde una nueva perspectiva la incidencia de la protección de datos en los más diversos sectores profesionales y empresariales, al establecer exigencias y principios en materia de protección de datos adaptados a la realidad propia del mundo empresarial y profesional; y por otra, el texto facilita el deseable equilibrio que debe presidir su aplicación con el irrenunciable avance social, económico y empresarial[5].

Así pues, y en relación con el tratamiento de la información personal en el ejercicio profesional, el abogado se enfrenta a nuevos retos, propios de la sociedad de la información y de su imparable avance en todos los sectores profesionales y sociales. En este contexto legal, la profesión jurídica debe ofrecer respuesta, entre otras, a las siguientes cuestiones: qué ámbitos organizativos y de gestión deben reformularse en un despacho de abogados para cumplir con la exigencia legal de protección de datos personales; cuál es la capacidad de respuesta o actuación ante una incidencia o problema legal en el tratamiento de datos personales y, por último, está el abogado o el despacho profesional preparado para enfrentarse a posibles denuncias ante la Agencia Española de Protección de Datos por actuaciones ilícitas en el tratamiento de la datos personales. Cierto es, sin embargo, que para resolver estas incertidumbres jurídicas, el abogado debe tomar conciencia de la importancia legal y social de la protección de datos personales, y valorar la seguridad de la información no solo como una cuestión de reputación e imagen, o de índole patrimonial, ante el temor a enfrentarse a un posible perjuicio económico. Por el contrario, debe conocer la normativa de protección de datos que le obliga legalmente a cumplir un conjunto de principios y derechos en su actividad profesional como abogado, y en consecuencia, adaptar su actividad y la prestación de sus servicios a los principios de protección de la información personal presentes en la normativa española y europea.

Y a esta realidad normativa pronto se sumará la nueva legislación europea de protección de datos personales, que establecerá, un marco normativo uniforme, integral y sólido para la garantía de los derechos de los ciudadanos a la tutela de sus datos personales. El breve análisis que tendremos oportunidad de avanzar sobre las novedades más destacadas de este Reglamento europeo nos permitirá descubrir si, como pronostican algunos expertos, nos encontramos ante un texto moderno que se ocupará de los retos de la globalización mediante instrumentos flexibles que facilitan el desarrollo de las empresas en un entorno internacional, garantizando al mismo

[4] Última modificación por Ley 2/2011, de 4 de marzo, de Economía sostenible. BOE nº 55, de 5 de marzo de 2011, pp. 25033-ss.

[5] Por todos, R. MARTÍNEZ MARTÍNEZ, "El Real Decreto 1720/2007, de 21 De diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Aspectos clave", *Revista Jurídica de Castilla y León*, núm. 16, 2008, pp. 257-293.

tiempo los derechos de los ciudadanos[6]; o si por el contrario, como lamentan otros muchos, el legislador europeo, encontrará serias dificultades para alcanzar un consenso en materias tan sensibles y controvertidas como el derecho a la supresión o el movimiento internacional de datos personales, lo que impedirá aprobar un nuevo texto europeo a medio plazo[7].

III. EL ABOGADO ANTE LA PROTECCIÓN DE DATOS PERSONALES

1. El abogado como responsable del tratamiento de datos personales. A propósito del modelo de despacho profesional

La problemática que afecta a los despachos de abogados en su esfuerzo por adaptarse y aplicar la normativa española de protección de datos personales no puede explicarse sin antes examinar los diferentes modelos organizativos en que se estructuran en la actualidad los profesionales del derecho. En efecto, el modelo de despacho profesional alcanza una especial trascendencia, habida cuenta que la fórmula escogida condicionará la delimitación legal del responsable del fichero y sus correspondientes obligaciones en el ámbito de la protección de datos.

Puede decirse que hasta fechas recientes, con carácter general, el despacho de abogados se organizaba como sociedad civil. No obstante, superados los iniciales recelos ante una organización empresarial de los despachos, viene siendo frecuente que las firmas de abogados se constituyan como sociedades mercantiles, cooperativas o como agrupaciones de interés económico. De esta forma, pueden distinguirse dos modelos de despachos profesionales: por una parte, los denominados "despachos colectivos" en los que se comparte un espacio común, unos servicios e incluso un nombre comercial o corporativo, pero se mantiene independencia sobre los ingresos y las respectivas carteras de clientes; y por otra, los despachos organizados como empresa, donde los profesionales son considerados trabajadores por cuenta ajena, los clientes, con independencia de quién los aporta, contratan sus servicios con la empresa, y no con el profesional. Bien es verdad, la Ley 2/2007, de 15 de marzo, que regula las sociedades profesionales, ha introducido un nuevo modelo profesional de despacho, las "sociedades profesionales", entendidas aquellas entidades que tienen por objeto social el ejercicio común de una actividad profesional y a las cuales les son atribuidos los derechos y obligaciones inherentes al ejercicio de la actividad profesional, como titulares de la relación jurídica establecida con el cliente[8].

Así, en una inicial aproximación, puede concluirse que si el responsable del tratamiento es quien decide sobre la finalidad, contenido y uso del tratamiento, en el ejercicio profesional de la abogacía, será responsable del tratamiento, quien aparezca como titular de la relación jurídica establecida con el cliente[9]. No obstante, cuando varios abogados compartan un mismo espacio común, unos servicios y el nombre comercial del despacho, pero manteniendo independencia económica, cada uno de ellos actuará como responsable del tratamiento que efectúe y, por ello, puede decirse que habrá tantos responsables del tratamiento como abogados integran el despacho

---

[6] Es de esta opinión V. REDING, "Protección de la privacidad en un mundo conectado. Un marco europeo de protección de datos para el siglo XXI", en J. PÉREZ y E. BADIA (coords), *El debate de la privacidad y seguridad en la red: regulación y mercados,* Ariel/Telefónica, Madrid, 2012, pp. XVII-XXV.

[7] Así se expresa R. Martínez, al considerar que" Otra cosa es ver si esta norma prospera porque realmente está muy atascada en su gestación y negociación. Hay que darse cuenta que es una gran novedad que la UE quiera regular de forma homogénea un derecho fundamental; hay expertos que cuestionan incluso que la propia UE pueda tener esa competencia parar regularlo". Cfr. Texto íntegro en http://www.lawyerpress.com/news/2013_08/0108_13_001.html (última consulta: 10/06/2014).

[8] Ley 2/2007, de 15 de marzo, de sociedades profesionales. BOE nº 65, 16 de marzo de 2007. Artículo 1.1º Definición de las sociedades profesionales: "Las sociedades que tengan por objeto social el ejercicio en común de una actividad profesional deberán constituirse como sociedades profesionales en los términos de la presente Ley.". Se define "actividad profesional" como aquella para cuyo desempeño se precisa titulación universitaria oficial, o titulación profesional para cuyo ejercicio sea necesario acreditar una titulación universitaria oficial, e inscripción en el correspondiente Colegio Profesional.

[9] M.A. DAVARA RODRÍGUEZ, *Guía práctica de protección de datos para abogados*, Editorial DaFeMa, Madrid, 2004.

colectivo[10]. Siguiendo lo dispuesto en el RLOPD, en los ficheros en los que exista más de un responsable, "cada uno de ellos deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero" (art. 57). Aunque inicialmente pudiera interpretarse que nos hallamos ante el tratamiento de datos personales en un despacho colectivo de abogados, lo cierto es que el fichero de un despacho colectivo de abogados no puede calificarse como un fichero con varios responsables, porque cada abogado, con actividad profesional independiente, responderá de sus propios ficheros de asuntos y deberá garantizar de forma adecuada el tratamiento de datos personales para impedir el acceso y uso de los datos a quienes no se encuentren autorizados[11].

Ahora bien, en los despachos colectivos, desde el punto de vista de la protección de datos personales, el denominado fichero de asuntos (datos de clientes, datos de abogados, expedientes, etc.) responde a una estructura mixta: por una parte, se presenta en formato papel, con las actuaciones y diferentes documentos escritos; en tanto que otra parte de los datos de dicho expediente se hallarán informatizados, esto es, nos encontramos ante un fichero "combinado". Los abogados del despacho colectivo deberán asumir su condición de responsables del fichero o del tratamiento integrado con los datos personales que utilicen para resolver los asuntos de sus propios clientes y a tal efecto, deberán cumplir con las obligaciones que se establecen en la LOPD y en el Reglamento, algunas de las cuales tendremos ocasión de analizar posteriormente.

Por el contrario, cuando la actividad se ejerce desde una firma de abogados, que actúa como empresa y adopta forma societaria, aquélla se constituye en titular de la relación jurídica con el cliente y por ende, será considerada responsable del fichero o del tratamiento. Desde una perspectiva organizativa, parece más sencillo dar cumplimiento a la normativa de protección de datos en este último caso; por tanto, la existencia de un único responsable, la posibilidad de establecer diferentes funciones y accesos en materia de protección de datos y el uso de las autorizaciones delegadas facilitarán, sin duda, la gestión de la protección de datos personales en la organización de una firma de abogados. Claro que ello no impide que puedan presentarse diversas problemáticas propias de la dinámica profesional del abogado; así, por ejemplo, plantea importantes dudas el tratamiento de datos personales en los asuntos en curso de los profesionales que se incorporen a la firma con cartera propia de clientes. Pueden adoptarse a este respecto dos soluciones: primera, que el abogado mantenga su condición de responsable del tratamiento de la información personal relativa a sus asuntos, circunstancia que no resulta satisfactoria ni práctica, porque no responde a la real situación que su incorporación ha generado; y segunda, que se arbitren procedimientos para que desde el momento de su incorporación se traslade la condición de responsable del tratamiento a la propia firma. Se propone para resolver este inconveniente la aplicación del artículo 19 del RLOPD, de suerte que "en los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre"[12]. Así las cosas, pudiera interpretarse que en el supuesto anteriormente se produce una modificación en la titularidad del responsable, de forma análoga a lo que acontece en una operación mercantil o en una aportación o transmisión de negocio; pero, se admita o no dicha lectura, lo cierto es que no podrá eludirse el deber de información dispuesto en el artículo 5 LOPD

[10] Se recomienda entonces que cada abogado proceda a la inscripción de los ficheros respecto de lo que los que actúa como responsable. Cada abogado deberá inscribir el fichero a su nombre. Así se interpreta por J. ÁLVAREZ HERNANDO, *GUÍA PRÁCTICA SOBRE PROTECCIÓN DE DATOS. Cuestiones y Formularios,* Lex Nova, Valladolid, 2011, pp- 377-ss.

[11] El futuro Reglamento europeo en su art. 24 contempla la posibilidad de corresponsabilidad del tratamiento, cuando varios responsables determinen conjuntamente los fines y los medios del tratamiento de datos personales; determinarán también cuáles son sus responsabilidades respectivas en el cumplimiento de las obligaciones y, en particular los procedimientos y mecanismos para el ejercicio de derechos del interesado.

[12] J. VERDAGUER LÓPEZ, "Tratamiento de datos personales en función del tipo de despachos", *Revista IURIS,* núm. 129, 2008, pp. 32-36.

y, conforme prevé el procedimiento previsto en el artículo 14 del RLOPD, se solicitará el consentimiento tácito, siempre y cuando aquél no deba ser expreso de conformidad con la LOPD.

En otro orden de consideraciones, puede ocasionar importantes complicaciones en el ámbito de la protección de datos la práctica habitual de la profesión jurídica de recabar colaboración externa al propio despacho de abogados, en aquellos casos en que los asuntos se trabajan de forma conjunta, con la participación tanto de profesionales externos como de miembros del propio despacho. En estas situaciones se recomienda establecer cautelas o protocolos desde la perspectiva de la protección de datos personales; así, por ejemplo: delimitar correctamente las respectivas obligaciones legales, identificar la cesión de datos personales al colaborador o la actuación de éste como encargado del tratamiento, la limitación y restricción en el acceso a los datos y al expediente, definir dónde tendrá lugar la actividad de colaboración y por tanto, la custodia y responsabilidad en relación con los soportes donde conste la información personal (en la sede de la firma o en su propio despacho), y finalmente, cuáles serán las medidas de seguridad que deban adoptarse y a quién corresponde dicha adopción.

Finalmente, cuando el despacho profesional se organiza como sociedad profesional dos son los aspectos que deben destacarse a partir de la aprobación de la Ley 2/2007, de 15 de marzo, de sociedades profesionales, en relación con la normativa de protección de datos personales, a saber: en primer lugar, a propósito de la condición de responsable del tratamiento, siempre corresponderán a la sociedad profesional los derechos y obligaciones inherentes al ejercicio de la actividad profesional como titular de la relación jurídica establecida con el cliente; de no ser así, nos hallaríamos ante una sociedad de intermediación o de medios que, carecerá de la condición de responsable del tratamiento al no ser titular de la relación jurídica con el cliente, y se trasladará dicha condición a los abogados que actúan a título individual con sus clientes; y en segundo lugar, cuando en la sociedad profesional los socios aportan sus respectivas carteras de clientes y asuntos, será igualmente la sociedad quién actúe como titular de la relación jurídica con el cliente, y en consecuencia, tendrá la consideración de responsable del tratamiento de la información personal.

2. Las obligaciones legales del responsable del tratamiento de datos personales en el despacho de abogados

Toda vez que se ha delimitado la figura del responsable del tratamiento de datos personales en los despachos colectivos y en las firmas de abogados, a continuación se examinarán las principales obligaciones que deben cumplir como responsables de un tratamiento de datos personales los despachos de abogados. A este respecto, con carácter general, señala la Agencia Española de Protección de Datos (en adelante AEPD) que "Sobre el responsable del fichero recaen las principales obligaciones establecidas por la LOPD y le corresponde velar por el cumplimiento de la Ley en su organización", en especial el responsable debe[13]:

a) Notificar los ficheros ante el Registro General de Protección de Datos para que se proceda a su inscripción.

b) Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.

c) Garantizar el cumplimiento de los deberes de secreto y seguridad.

d) Informar a los titulares de los datos personales en la recogida de éstos.

e) Obtener el consentimiento para el tratamiento de los datos personales.

[13] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía del responsable de ficheros*. Véase en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf (última consulta: 01/06/2014).

f) Facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

g) Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto en la LOPD.

h) Cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que le sea de aplicación.

2.1. Las obligaciones formales: notificación e inscripción de los ficheros

De conformidad con el artículo 55.2 del RLOPD "Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar: la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos".

Desde la perspectiva de la protección de datos personales la primera obligación legal en un despacho de abogados es la notificación de los ficheros (clientes, proveedores, trabajadores, candidatos) a la AEPD para su inscripción en el Registro General de Protección de Datos. Esta obligación formal de inscripción ha de ser previa a la utilización de los ficheros y al inicio del tratamiento. En todo caso, la notificación se referirá a cuantos ficheros recojan información personal en el despacho, con independencia de cuál sea su naturaleza o formato, esto es, automatizados, manuales o combinados (Véase RAEPD R/00997/2010, de 7 de mayo de 2010).

Define el RLOPD como fichero "todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso" (artículo 5.1º k) y como fichero no automatizado "todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica"(artículo 5.1º n). Así mismo, exige el artículo 58 de la citada norma que "La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55". En su caso, además, cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

Constituye infracción leve, conforme al artículo. 44.2 LOPD[14], no remitir a la AEPD las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo y, no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos. A continuación, el artículo 45.1 LOPD señala que "Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros" (Véase RAEPD R/00209/2008, de 28 de febrero de 2008).

[14] Cfr. Ley 2/2011, de 4 de marzo, de Economía Sostenible. *Boletín Oficial del Estado*, 5 de marzo de 2011, nº 55, p. 25033.

Ahora bien, si la última versión del Reglamento europeo de protección de datos prospera, no deberá procederse a la notificación de los ficheros a la autoridad de control, y esta obligación se sustituye por la exigencia de conservar la documentación, actualizada periódicamente, que sea necesaria para cumplir los requisitos que se establecen en el texto (art.28), al tiempo que se podrá solicitar un certificado o sello de confianza a la autoridades de que certifique que el tratamiento de datos personales se efectúa de conformidad con el presente Reglamento (art. 39 1 bis).

2.2. Los principios de protección de datos personales en el ejercicio de la abogacía. El deber de secreto profesional

Con carácter general, dispone la LOPD en su artículo 4.1º que "Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". Así mismo, el citado artículo en su apartado segundo apunta que "Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos". Y finalmente, el tercer apartado recuerda que "Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado".

En definitiva, el abogado o el despacho de abogados deben asegurarse que obtienen los datos de carácter personal exclusivamente para cumplir con las finalidades determinadas, explícitas y legítimas para las que son recabados, de suerte que los datos personales solicitados sean adecuados, pertinentes y no excesivos en relación con dichas finalidades. Además, los datos de carácter personal tienen que ser exactos y puestos al día, reflejando la situación actual del afectado; corresponde, en los términos señalados por la LOPD, proceder de oficio al titular del fichero para cancelar y sustituir los datos personales cuando éstos resulten ser inexactos, en todo o en parte, o incompletos; en su caso, los datos de carácter personal deberán cancelarse cuando no sean necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados (art. 4.5 LOPD). En este sentido, tuvo la oportunidad de pronunciarse la AEPD a propósito de los datos personales que los abogados revelaban a los Colegios Profesionales como medio de justificación de su actuación de oficio, a los efectos de percibir la correspondiente remuneración por dichos servicios. Concluyó la AEPD que si bien deben presentarse la primera hoja de autos y sentencias junto con el justificante de intervención procesal debidamente sellado, deben ocultarse los datos personales que revelen información sobre el fondo del asunto, por entender que es innecesario que el correspondiente Colegio de Abogados disponga de dicha información a los citados efectos[15].

En el ejercicio de la abogacía, la exigencia legal de deber de secreto representa una máxima irrenunciable, no en vano el vínculo de confianza que se establece entre el cliente y el abogado determina que aquél revele información sensible y datos con la seguridad que le merece el deber de su represente de mantenerlos en la más estricta confidencialidad[16]. Y así, siguiendo la opinión de ANDINO LÓPEZ, este deber se configura en la legislación española no como un

[15] Véase Informe AEPD 0170 /2008.

[16] Adquieren especial relevancia las afirmaciones del TC a propósito del reconocimiento de un deber de secreto profesional amparado constitucionalmente en el art. 24.2 CE, y por el cual, "la confianza y la confidencia son, pues, dos requisitos inseparables del asesoramiento técnico del abogado defensor, forman parte del 'núcleo esencial' del derecho de defensa y no concurren cuando se impone un abogado que no aporta al justiciable la intimidad imprescindible para que haya una comunicación recíproca entre ambos que, además, debe quedar reservada, pues de lo contrario, no se manifestaría: quedaría coartada, limitada y cercenada, lo que significa una mutilación de la propia asistencia letrada". Véase STC 110/84, de 26 de noviembre, BOE núm. 305, de 21 de diciembre.

derecho fundamental en sí mismo, sino como garantía de otros derechos fundamentales de terceros[17].

Ofrece una definición de secreto profesional, en el ámbito propio del ejercicio profesional de la abogacía, el Estatuto General de la Abogacía Española en vigor, que en su artículo 23.1º prevé que "... los abogados deberán guardar secreto de todos los hechos o noticias que conozcan por razón de cualquiera de las modalidades de su actuación profesional, no pudiendo ser obligados a declarar sobre los mismos", al tiempo se señala en su artículo 42 que "son obligaciones del abogado para con la parte por él defendida..., el cumplimiento de la misión de defensa que le sea encomendada con el máximo celo y diligencia y guardando el secreto profesional"[18]. Abundando en lo expresado, el Código Deontológico aprobado en 2002 por el Consejo General de la Abogacía española en su artículo 5.2º explica que "el deber y derecho al secreto profesional del abogado comprende las confidencias y propuestas del cliente, las del adversario, las de los compañeros y todos los hechos y documentos de que haya tenido noticia o haya recibido por razón de cualquiera de las modalidades de su actuación profesional"[19]. Ello no obstante, el Consejo general de la Abogacía Española aprobó en el pleno celebrado el 12 de junio de 2013 un nuevo texto, que ha sido remitido al Ministerio de Justicia para la correspondiente tramitación y aprobación definitiva por el Gobierno[20].

La propia LOPD en su artículo 10 establece para el responsable del fichero y para quienes intervengan en cualquier fase del tratamiento de datos personales la obligación de "secreto profesional respecto de los mismos y el deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo". En el ámbito de la protección de datos personales, la vulneración del deber de secreto, constituye una infracción grave conforme a la nueva redacción del artículo 44.3 de la LOPD, que puede ser sancionada con una multa que oscila desde los 40.001 a 300.000 euros (art. 45.2 LOPD).

Siguiendo las reflexiones de LLORENTE GUILLÉN[21], en las que examina los conceptos de secreto profesional y de deber de secreto en el ámbito de la LOPD, puede concluirse que si bien la cualidad del deber de reserva es absoluta, el deber de secreto cede en el cumplimiento de una obligación o deber legal de suministrar datos[22]. Señala, así mismo, la autora que el origen de ambas obligaciones diferencia igualmente a ambos deberes, ya que si bien la obligación recogida en la LOPD sólo se origina cuando los datos suministrados se incorporan a un fichero, automatizado o no, el secreto profesional nace desde el mismo momento en que la información se revela por el cliente al abogado o se tiene conocimiento por cualquiera otra actuación profesional. A juicio de la citada autora, la condición de confidencialidad que debe tener la información sujeta

---

[17] J.A. ANDINO LÓPEZ, *Efectos de la vulneración del secreto profesional del abogado en el proceso civil.* Facultat de Dret. Universitat de Barcelona, Barcelona, 2013, pp. 103-107.

[18] Cfr. RD 658/2001, de 22 de junio, por el que se aprueba el Estatuto General de la Abogacía Española. Boletín Oficial del Estado, de 10 de julio de 2001, nº 164, pp. 24913-24932.

[19] Señala así mismo, el Código Deontológico en su artículo 5 que "en todo caso, el abogado deberá hacer respetar el secreto profesional a su personal y a cualquier otra persona que colabore con él en su actividad profesional"; estableciéndose, además, que "estos deberes de secreto profesional permanecen incluso después de haber cesado en la prestación de los servicios al cliente, sin que estén limitados en el tiempo". Véase Código deontológico, adaptado al Estatuto General de la Abogacía Española, aprobado por Real Decreto 658/2001, de 22 de junio, y aprobado en el Pleno de 27 de septiembre de 2002.

[20] En el Estatuto General de la Abogacía, pendiente de aprobación por el Gobierno, se señala en el art. 17.4 que las comunicaciones confidenciales deberán enviarse encriptadas y con forma electrónica segura, siempre que las circunstancias del cliente lo permitan. Se define el secreto profesional como "… el deber y el derecho de guardar secreto de todos los hechos o noticias que conozca por razón de cualquiera de las modalidades de su actuación profesional, no pudiendo ser obligado a declarar sobre ellos" (art. 22); y se señala igualmente que el ámbito de este derecho-deber comprende "… todos los hechos, comunicaciones, datos, informaciones, documentos y propuestas que, como Abogado, haya conocido, emitido o recibido en su ejercicio profesional" (art. 23.1).

[21] B. LLORENTE GUILLÉN, "Análisis del deber de secreto de la Ley orgánica de protección de datos en relación con el secreto profesional de los abogados", *Anuario de la Facultad de Derecho. Universidad de Alcalá de Henares,* núm. 2, 2009, pp. 503-514.

[22] Véase STS Sala 3ª, Sección 7ª, de 27 de septiembre de 2002.

al secreto profesional de los abogados, no es necesaria en el supuesto de los datos de carácter personal, vulnerándose éste por la mera revelación de cualquier tipo de dato personal contenido en un fichero o tratamiento. En cuanto a las similitudes, ambos deberes, presentan carácter vitalicio, pues ambos subsisten durante toda la vida del profesional, de suerte que persisten aún después de finalizar la relación con el cliente o el interesado o con posterioridad a causar baja en la profesión. Y por último, según se desprende de la LOPD, el deber de secreto no sólo obliga al responsable del fichero o al abogado, sino que se extienden también a quienes con ellos colaboren o tengan conocimiento de los datos e informaciones personales; bien entendido que conforme al denominado "principio de mínimo privilegio", cada persona sólo deberá acceder a los datos personales precisos para el ejercicio de su actividad (arts. 89 y 91 RLOPD).

2.3. El ejercicio de derechos por los interesados. En especial, la prestación del consentimiento y el deber de transparencia

Como ya tuvo ocasión de proclamar el Tribunal Constitucional en la célebre Sentencia 292/2000, los derechos del interesado constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y garantizan a la persona el control sobre sus propios datos personales[23]. Abundando en lo expresado, explica el artículo 23 RLOPD que "Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado". Con todo, los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro (art. 24 RLOPD). Se afirma igualmente que deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos, sin que en ningún caso genere ingresos adicionales para el responsable del tratamiento ante el que se ejercitan.

El Reglamento intenta reforzar las garantías legales en el ejercicio de los derechos de los afectados, obligando a los responsables del fichero o del tratamiento a disponer procedimientos sencillos y «gratuitos» para el ejercicio de los derechos ARCO. Es por ello, que se declaran no conformes a la normativa los supuestos en los que se exija el envío de cartas certificadas, la utilización de servicios de telecomunicaciones que impliquen tarificación adicional o cualesquiera otros que impliquen un coste excesivo para el afectado (art. 14.4º y 5º RLOPD).

Por todo ello, el despacho de abogados deberá habilitar un procedimiento sencillo y gratuito para el ejercicio de estos derechos; por lo que, en su caso, si dispone de servicio de atención al cliente, podrá conceder la opción de su ejercicio a través de dicho servicio. Desde una perspectiva práctica, entre las diversas posibilidades que la normativa contempla, y que pueden ponerse a disposición de los interesados por el responsable del fichero destaca la facultad de habilitar una cuenta de correo electrónico, o un número de teléfono que con carácter exclusivo atiendan a estas comunicaciones. Ello no obstante, ante la petición de ejercicio de los derechos ARCO por parte del afectado, el despacho deberá proporcionar una respuesta en el plazo y con los requisitos que establece el Reglamento, tanto si se dispone de datos personales del solicitante como si no constan en los ficheros datos personales del afectado (art. 23 y ss RLOPD)[24].

---

[23] Ahora bien, como nos recuerda la STC 290/2000 "... el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, FJ 7; 196/1987, de 11 de diciembre, FJ 6; y respecto del art. 18, la STC 110/1984, FJ 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental". Cfr. STC 290/2000, de 30 de noviembre, BOE núm. 4, de 4 de enero de 2001.

[24] La Resolución de la AEPD R/00220/2008 de 3 de marzo de 2008, en un procedimiento de tutela de derechos, examina el supuesto de un despacho de abogados que no atendió correctamente la solicitud de cancelación de una ex empleada, al mantener su fotografía en la página web del despacho, una vez que su relación laboral con la firma de abogados ya había concluido.

En relación con la exigencia de recabar el consentimiento del interesado, con carácter general y previo al tratamiento de los datos de carácter personal del cliente, proveedor o trabajador, se deberá obtener el consentimiento informado para todo tratamiento, y para las concretas finalidades legítimas que motivan su recogida, salvo que la ley disponga otra cosa. Igualmente, a estos efectos, se recomienda establecer protocolos y normas en los procesos de atención al cliente y en la aceptación de los encargos profesionales. En efecto, es conveniente incluir en la propuesta de servicios, contrato u hoja de encargo, la cláusula informativa sobre protección de datos de carácter personal, con los requisitos exigidos en el artículo 5 LOPD.

Por otra parte, en los despachos de abogados son frecuentes las prácticas de marketing y promoción de sus servicios legales, que permiten asegurar una publicidad entre sus clientes y proveedores, y distinguirse por la especialización jurídica del despacho en un concreto ámbito o materia legal. Para ello, es habitual que se proceda al envío de correspondencia, correos electrónicos, informando sobre la organización de cursos, jornadas, o la publicación de obras monográficas y la organización de encuentros temáticos. Siguiendo las previsiones del artículo 46 RLOPD, si el despacho de abogados decidiera realizar por sí un actividad publicitaria de sus productos o servicios entre sus clientes "será preciso que el tratamiento se ampare en alguno de los supuestos contemplados en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre". En estos casos, las medidas de seguridad se adoptarán en función del medio que se utilice para la promoción de los servicios y de los destinatarios de los mismos; así, si se trata de un envío postal ordinario, en principio, los datos de carácter personal que se utilicen para determinar los destinatarios del envío procederán de la base de clientes o habrán sido obtenidos de forma legítima o de fuentes accesibles al público, por lo que salvo que el interesado haya manifestado su oposición a dicho tratamiento no hay dificultad legal para la utilización de los datos personales. Sin embargo, si se procede a efectuar un envío por correo electrónico o sistema equivalente, de conformidad con la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico (art. 21 y ss.), se debe obtener el consentimiento previo, bien se trate de personas físicas o jurídicas, salvo que exista una relación contractual previa, y siempre que no conste la oposición explícita del interesado a dicho tratamiento[25]. Abundando en lo expresado, confirma la Audiencia nacional la sanción impuesta por la AEPD a un despacho de abogados por envío de comunicaciones promocionales, pues si bien el interesado prestó el consentimiento para dicho tratamiento, no se establecía un procedimiento específico para la oposición al tratamiento de dichos datos personales con fines promocionales[26]. Más recientemente ha declarado este mismo Tribunal que "la legitimidad de la posesión de los datos por parte de una concreta empresa no obsta a la posterior necesidad del recabado de un consentimiento específico para la remisión de comunicaciones comerciales. (…). Es decir, se puede haber obtenido la dirección de correo de forma licita pero eso no legitima para el envío de comunicaciones comerciales"[27].

2.5. Las medidas de seguridad de los ficheros: la evaluación del impacto en la protección de datos personales

Constituye una obligación legal la implantación de cuantas medidas de seguridad sean precisas atendiendo a la naturaleza de la información que se trate en el ejercicio profesional; y así, como mínimo exigible, cualquiera responsables que traten datos de carácter personal deberán adoptar e implantar un "documento de seguridad" (art. 9 LOPD y art. 81 RLOPD).

La elaboración del documento de seguridad del despacho, que recoge todas las medidas técnicas y organizativas previstas en la normativa, se podrá llevar a cabo en un único documento para todos los ficheros o en documentos separados para cada fichero o para grupos de ficheros. Dicho documento de seguridad será de obligado cumplimiento para el personal con acceso a los sistemas de información. Se recomienda en el caso de despachos colectivos, que cada abogado

[25] Véase AEPD. R/01948/2010, de 16 de septiembre de 2010.
[26] Cfr. Sentencia de la Audiencia Nacional de 14 de noviembre de 2007 (Rec. 78/2006).
[27] Cfr. Sentencia de la Audiencia Nacional, de 23 de julio de 2013 (Rec. 371/2012).

como responsable del tratamiento disponga de su documento de seguridad, que deberá permanecer siempre actualizado.

El Reglamento ha precisado el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad. Así, respecto al tratamiento de datos por cuenta de terceros, se establece que en el documento de seguridad deberá establecerse la identificación de los ficheros o tratamientos que sean tratados en concepto de encargado de tratamiento. Además, si los datos de un fichero se tratan de forma exclusiva en los sistemas del encargado, esta circunstancia también deberá mencionarse en el documento de seguridad del responsable.

Con relación a estas dos obligaciones, la inscripción de ficheros y la elaboración del documento de seguridad, es interesante destacar la Resolución R/00209/2008, de 28 de febrero de 2008, en la que la AEPD impone una multa a un abogado por no haber adoptado las correspondientes medidas de seguridad en el fichero automatizado con datos personales de sus clientes, pese a disponer de documento de seguridad. Apunta con acierto Pérez Gómez que en los casos de adaptación de la actividad profesional al régimen jurídico de protección de datos corresponde establecer un estándar de seguridad que además de facilitar la adaptación a la LOPD, constituya un paso previo y necesario a la implantación de un sistema de gestión de seguridad de la información (SGSI)[28].

Por su parte, prevé el RLOPD que todos los ficheros o tratamientos de datos de carácter personal adoptarán las medidas de seguridad calificadas de nivel básico (art. 81.1º RLOPD). En su caso, y dependiendo de la naturaleza de los datos, se adoptarán con carácter acumulativo el nivel medio o alto de seguridad, según corresponda. Por tanto, en consideración al tipo de asuntos y procedimientos que tramite cada despacho, y en consecuencia, en atención a la naturaleza de la información personal que se maneje se determinará el nivel de seguridad que deberá adoptarse, "…con independencia de cuál sea su sistema de tratamiento", automatizado o no (art. 79 RLOPD). Con carácter general, los ficheros o tratamientos relativos a la comisión de infracciones administrativas o penales y aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, deberán implantar el nivel de seguridad medio (art. 81.2 RLOPD); así, por ejemplo, los ficheros de candidatos, estudiantes en prácticas, procesos de selección y currículums que se entregan al despacho en procesos de selección o de forma espontánea. Por otra parte, conforme al artículo 81.3 RLOPD, además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán a los ficheros o tratamientos que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, y a aquéllos que contengan datos derivados de actos de violencia de género. No obstante, aquellos despachos cuya actividad se oriente a reclamaciones penales y civiles de responsabilidad médica o accidentes de tráfico incorporan a sus ficheros y tratamientos datos personales especialmente protegidos de salud, por lo que les corresponderá adoptar un nivel de seguridad alto.

Finalmente, no se presta por las organizaciones especial atención en materia de protección de datos personales a la formación e información que debe ofrecerse al personal que desempeña sus servicios o colabora con el despacho de abogados, y que sin ser responsable del fichero, sin embargo, por exigencias de su trabajo accede y trata información personal[29]. Abundando en lo expresado, el propio RLOPD exige que en el documento de seguridad se haga constar: el personal al que afecta el documento, sus funciones y su actuación con los datos; para ello, se establecerá lo que se conoce como "principio de mínima intervención", esto es, que cada persona únicamente

[28] E. PÉREZ GÓMEZ, "La protección de datos de carácter personal en un despacho de abogados", *Diario La Ley*, núm. 7524, Año XXXI, 9 de Dic. de 2010.

[29] Davara Rodríguez señala que la responsabilidad del abogado por el tratamiento de los datos personales en su despacho le obliga a formar e informar a las personas que accedan a los datos personales; apercibiéndoles, en su caso, de las responsabilidades en que puedan incurrir cuando se produce un tratamiento inadecuado de la información personal. M. A. DAVARA RODRÍGUEZ, *Decálogo del Abogado de Protección de Datos*, La Ley, Madrid, 2007, pp.95-96.

acceda a los datos personales que necesite en atención a sus propias funciones. En efecto, declara el RLOPD que "El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información" (art. 88.1 RLOPD). Deberá en dicho documento deberán definirse "funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros" (art. 88.2 RLOPD). De igual forma, se obliga al responsable del fichero o del tratamiento a adoptar "las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento" (art. 89.2 RLOPD).

Como novedad, los despachos de abogados en un futuro próximo tendrán que considerar que la entrada en vigor del Reglamento europeo incorpora para los responsables del tratamiento y los encargados la obligación legal de realizar una "evaluación del impacto en la protección de datos personales" en los supuestos previstos legalmente (arts. 32 bis y 33), tales como tratamiento de datos sensibles, o de elaboración de perfiles con efectos jurídicos… En la actualidad, no existe conforme a la legislación española dicha obligación, si bien la AEPD ha iniciado y abierto el proceso de preparación de una Guía[30], actualmente en borrador, para la evaluación del impacto en la protección de datos personales como medio fundamental para el análisis de los riesgos del tratamiento de datos en la privacidad de las personas y la adopción preventiva de medidas de seguridad adecuadas a cada tratamiento de datos personales.

IV. EL EJERCICIO PROFESIONAL Y LA UTILIZACION DEL "CLOUD COMPUTING" EN LOS DESPACHOS DE ABOGADOS

En expresión de la AEPD, puede definirse el "cloud computing" como "el modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables, como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios que pueden set rápidamente asignados y libertados con una mínima gestión por parte del proveedor de servicios"[31]. Este modelo de prestación de servicios[32], se caracteriza porque los recursos, información, documentos son accesibles a través de la red, y mediante diversos dispositivos de usuarios tales como teléfonos móviles, ordenadores portátiles o PDAs; igualmente, también los recursos (almacenamiento, memoria, ancho de banda,…) son compartidos por varios usuarios.

Desde la perspectiva de un despacho de abogados, este modelo permite el acceso a un conjunto de servicios y aplicaciones informáticas como correo electrónico, almacenamiento de documentos, acceso a bases de datos, compartir documentos e informes con clientes o con otros profesionales… Fácilmente pueden advertirse las importantes e inmediatas ventajas que la contratación de este modelo de servicios reporta al ejercicio profesional de la abogacía. Así, no será preciso que el despacho de abogados disponga de personal informático propio para el mantenimiento de servidores y aplicaciones; por otro lado, el acceso a los servicios se encuentra disponible desde cualquier dispositivo, y desde cualquier lugar con conexión a internet, y es el

[30] En palabras de la AEPD la evaluación del impacto en la protección de datos constituye una herramienta esencial para"…la cuidadosa evaluación de los riesgos que para la privacidad de las personas tiene cualquier nuevo sistema que trate datos de carácter personal y, para ello, […] permite identificar y eliminar o mitigar estos riesgos en las primeras fase de diseño de un sistema. Así se aumenta la confianza entre los usuarios y se evitan costosos re-diseños y posibles daños a la imagen y a la economía de las organizaciones al producirse (o percibir que se producen) invasiones indebidas en la privacidad de las personas". Cfr. AEPD. *Guía para una evaluación del impacto en la Protección de Datos personales (borrador),* de marzo de 2014, pp.3-4.

[31] AEPD Y CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA, Informe: utilización del cloud computing por los despachos de abogados y la protección de datos de carácter personal. Véase texto íntegro en www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/junio/informe_CLOUD.pdf (última consulta: 06/06/2014).

[32] Para una información más completa véase P. Mell y T. Grance, "The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology", Special Publication 800-145, US Departament of Commerce, 2011.

proveedores de servicios quien asegura la disponibilidad de los recursos y la actualización permanente de servicios y aplicaciones.

Claro que como sucede siempre que nos encontramos ante cualquier avance tecnológico, son numerosas las dudes e incertidumbres jurídicas que acompañan a la implantación de este modelo de servicio[33]. A este respecto, la seguridad de la información personal, la garantía del secreto profesional en caso de los abogados, el escrupuloso cumplimiento de la legalidad en materia de protección de datos personales, los comprensibles temores a perder el control físico de la información personal tratada por el despacho de abogados y almacenada en la nube, y las dudas sobre la adopción de las adecuadas y necesarias medidas de seguridad de protección de datos personales.

Por todo ello, y a la vista el informe elaborado por la AEPD en colaboración con el Consejo General de la Abogacía Española, puede concluirse que son tres los aspectos que deben cuidarse especialmente por el despacho de abogados cuando adopta la decisión de contratar un servicio de "cloud computing", a saber:

a) Cuál es la responsabilidad de despacho en el tratamiento de datos personales y la normativa en vigor aplicable a dicho tratamiento.
b) Cómo debe preservarse la confidencialidad y seguridad de la información personal.
c) Los aspectos esenciales del contrato de servicios que deberá suscribir el despacho, desde la perspectiva legal y técnica.

A propósito de la desconfianza que genera la contratación de estos servicios, con carácter general y en lo que a la protección de datos se refiere, los problemas más significativos se identifican con la mayor exposición de los puntos de acceso; problemas con la segregación y aislamiento de datos personales; mayor número de elementos fuera del perímetro de seguridad del cliente; alto grado de concentración de información en una misma ubicación. No obstante, y como con acierto expone MORALES, contratar un servicio de *cloud* puede representar una oportunidad para mejorar la seguridad, si se realiza de forma adecuada y con un proveedor bien seleccionado[34]. Sin embargo, lo cierto es que la contratación de esta prestación de servicios, puede llegar a incrementar el riesgo de incidentes de seguridad de datos, de incorrecto tratamiento de los datos, o de fallos en la migración, retorno o destrucción de datos personales. En especial, como nos recuerda el citado autor, un riesgo específico será el posible incumplimiento de obligaciones sobre protección de datos de carácter personal; es por ello, que el Grupo de Protección de Datos del Artículo 29 ya señaló que el despliegue de los servicios de computación en la nube puede ocasionar riesgos para la protección de datos de carácter personal motivados por la falta de control sobre los datos o por una insuficiente información sobre el tratamiento realizado por el encargado (si tendrá lugar subtratamiento de la información, transparencia sobre el cómo, dónde y por quién los datos son tratados o en su caso, …)[35].

Respecto al tratamiento de la información en el *cloud* y el ejercicio profesional, debe tenerse presente en todo momento lo dispuesto por la normativa española, que conforme al art. 3 d) LOPD dispone que son responsables del tratamiento, aquellos a quienes corresponde la decisión sobre la finalidad, contenido y uso del tratamiento. Por ello, exige el art. 12 LOPD que se documente en un contrato que acredite el tratamiento de datos personales por cuenta de terceros, con la obligación por parte del encargado de seguir instrucciones del responsables del

[33] Dictamen CNS-57/2013 de la APDCAT (Autoritat Catalana de Protecció de Dades) en relación con la consulta de un Colegio de Abogados, sobre los riesgos que conlleva el uso de "Google Drive©", "Microsoft skydrive©" y "Dropbox©" en el ámbito profesional de las relaciones entre abogado y cliente, de 28 de marzo de 2014. Véase texto original en http://www.apd.cat/media/dictamen/ca_633.pdf#search="cloud" (última consulta: 06/06/2014).
[34] J. R. MORALES, "Cloud computing: riesgos corporativos e implicaciones jurídicas", *Actualidad Jurídica Aranzadi*, núm. 863, 2013, pp-3-4.
[35] Cfr. Informe Grupo de Protección de Datos del Artículo 29, Dictamen 5/2012 sobre la computación en la nube de 1 de julio de 2012.

tratamiento[36], y respetando la finalidad del tratamiento específicamente prevista en el contrato; y sin que en ningún caso pueda conservar dichos datos personales, que deberán destruirse o devolverse a la conclusión del contrato.

Por otra parte, a tenor de la propuesta de Reglamento Europeo de Protección de Datos, el despacho de abogados como responsable del tratamiento, "…elegirá un encargado del tratamiento que ofrezca garantías suficientes para implementar medidas y procedimientos técnicos y organizativos apropiados, de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento y garantice la protección de los derechos del interesado…" (art. 26.1). En todo caso, conforme expresa el texto de la Propuesta de Reglamento, "la realización del tratamiento por un encargado se regirá por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento" (art. 26.2), si bien el responsable y el encargado podrán determinar libremente sus respectivos papeles y tareas con respecto a los requisitos que deben cumplirse en el presente Reglamento. Destaca la previsión normativa europea por la cual, si un encargado del tratamiento desconoce o incumple las instrucciones del responsable del tratamiento o se convierte en parte determinante en relación con los fines y los medios del tratamiento de datos será considerado responsable del tratamiento con respecto a ese tratamiento (art. 26.4).

De todo lo expuesto se desprende que cuando el despacho de abogados adopte la decisión de contratar servicios de *cloud* deberá valorar como aspectos más relevantes para garantizar la legalidad del servicio y el cumplimiento de la normativa de protección de datos[37], por un lado, la pérdida de control sobre el tratamiento de la información personal y las consecuencias que ello representan; por otro lado, las problemáticas derivadas del movimiento internacional de datos personales[38] y posibles incidentes en materia de vulneración de derechos fundamentales, y por último, las dificultades jurídicas que presenta el tratamiento de datos por cuenta de terceros, y su acomodación a las normas nacionales y europeas[39].

V. APUNTES SOBRE EL REGLAMENTO GENERAL EUROPEO DE PROTECCION DE DATOS PERSONALES Y SU INCIDENCIA EN EL EJERCICIO PROFESIONAL DE LA ABOGACIA

Largo está siendo el peregrinar de las normas europeas de protección de datos personales hasta la reciente Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento general de protección de datos. Nadie duda hoy de la necesidad de adaptar y armonizar la dispersa, obsoleta, y en ocasiones, "invalidada"[40] normativa europea de protección de datos personales. Y en este proceso, en el que actualmente estamos inmersos, se encuentra más justificado que nunca, ante la inminencia de una nueva normativa europea que ofrezca la esperada respuesta al imparable avance tecnológico, detenernos brevemente a exponer los aspectos más controvertidos de la futura normativa europea de protección de datos personales, que desde luego tendrán también especial incidencia el tratamiento de datos personales por los despachos de abogados.

---

[36] A este respecto, el encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello (art. 21 RLOPD).

[37] Para un estudio en profundidad de las implicaciones legales del *cloud computing* en la protección de datos personales, R. MIRALLES, "*Cloud computing* y protección de datos", *Revista de Internet, Derecho y Política*, núm. 11, 2010, pp. 14-23.

[38] La localización del centro de proceso de la información constituye una cuestión jurídica fundamental. En efecto, la contratación de estos servicios podrá significar un movimiento internacional de datos personales; así, sucederá cuando la transmisión de los datos derivada de la prestación de los servicios de *cloud* se realice fuera Espacio Económico Europeo. Entonces se requiere con carácter general autorización del Director de la AED, salvo que las transmisiones se efectúen a Estados con "nivel de protección adecuado", o a entidades adheridas a los principios de Puerto Seguro (arts. 33 y 34 LOPD).

[39] Así lo expresa también Y. ADSUAR, "Cloud computing vs protección de datos de carácter personal", *Actualidad Jurídica Aranzadi,* núm. 846, 2012.

[40] Véase la Resolución del TJCE (Gran Sala), asuntos acumulados C-293-12 y C-594-12, de 8 de abril de 2014, por la que se invalida la Directiva 2006/24/CE sobre conservación de datos de tráfico.

Conforme el propio texto del Reglamento de protección de datos expresa, éste tiene por objeto:

> a) adaptar la protección de datos a las nuevas demandas del mundo digital, considerando que las disposiciones actuales se adoptaron cuando menos del 1 % de los europeos utilizaba Internet;
>
> b) evitar las actuales divergencias en la aplicación de las normas de 1995 por parte de los diferentes Estados miembros y velar por que los derechos fundamentales a la protección de datos personales se apliquen de manera uniforme en todos los ámbitos de las actividades de la Unión;
>
> c) aumentar la confianza del consumidor en los servicios en línea facilitando una mejor información con respecto a los derechos y a la protección de datos mediante la introducción del derecho a la rectificación, al olvido y a la supresión de los datos, derecho a la portabilidad de datos y de oposición;
>
> d) impulsar el mercado único digital reduciendo la fragmentación actual y las cargas administrativas.

Cabe esperar antes de finalizar el presente año, la aprobación definitiva del texto, habida cuenta de las últimas enmiendas al texto introducidas por el Parlamento europeo en marzo de este mismo año, y considerando que únicamente falta para la aprobación definitiva el visto bueno del Consejo de Ministros[41]. A pesar de ello, han sido numerosas las críticas que desde los más diversos sectores jurídicos se han presentado al texto, entre las principales objeciones destacan:

> a) La excesiva carga administrativa que el Reglamento prevé imponer a aquellos negocios que traten datos personales de más de 5000 usuarios; en especial, (art. 32 bis) las "evaluaciones de impacto" que constituyen el núcleo esencial de cualquier marco sostenible de protección de datos, al asegurar que las empresas sean conscientes desde el principio de todas las posibles consecuencias de sus operaciones de tratamiento de datos. Si las evaluaciones de impacto son exhaustivas, podrá limitarse esencialmente la probabilidad de que una operación vulnere la protección de los datos o invada la privacidad. Por consiguiente, las evaluaciones de impacto de la protección de datos deben tener en cuenta la gestión durante todo el ciclo de vida de los datos personales, desde la recogida y el tratamiento hasta la supresión, describiendo con detalle las operaciones de tratamiento previstas, los riesgos para los derechos y libertades de los interesados, las medidas previstas para abordar estos riesgos, las salvaguardias, las medidas de seguridad y los mecanismos para garantizar el cumplimiento del presente Reglamento (se introduce un nuevo considerando 71 bis).
>
> b) Se impone además (enmienda 39, considerando 63) la designación de un Delegado de Protección de Datos cuando la empresa procese datos personales de 5000 o más individuos en un período consecutivo de 12 meses.
>
> c) Las sanciones resultan desproporcionadas; la autoridad de control correspondiente impondrá al menos una de las siguientes sanciones: a) un aviso por escrito en casos de primer incumplimiento no deliberado; b) auditorías regulares del sistema de protección de datos; y c) Las sanciones administrativas oscilarán entre1.000.000 € o el 2% del volumen de negocios total de la empresa, hasta 100.000.000 € o el 5% del volumen de negocios global, prevaleciendo la cantidad que resulte superior.

[41] A este respecto, declaró la Presidencia Griega su voluntad de alcanzar un acuerdo para la adopción del texto en el primer semestre de 2014. Véase http://www.europarl.europa.eu/news/es/news-room/content/20140307IPR38204/html/La-Euroc%C3%A1mara-refuerza-la-protecci%C3%B3n-de-datos-de-los-europeos-en-la-era-digital (última consulta: 08/06/2014).

Ello no obstante, si el responsable del tratamiento o el encargado del tratamiento han obtenido un Sello Europeo de Protección de Datos de la autoridad de control correspondiente, las sanciones sólo serán impuestas en casos de incumplimiento intencionado o negligente.

d) Se lamenta que el legislador europeo haya optado por establecer un doble marco normativo en el ámbito de la protección de datos personales; estableciendo un marco general de la UE para la protección de datos, y Una Directiva que establece normas sobre protección de datos personales tratados con fines de prevención, detección, investigación y enjuiciamiento de delitos y otras actividades relacionadas con la justicia[42].

e) Y por último, si las iniciales versiones del texto se aproximan en mayor medida a la normativa española de protección de datos, debe lamentarse que las últimas revisiones del texto lo alejen de la normativa española, y acojan postulados y principios más propios de las normas germanas. Esta situación no viene sino a complicar y sembrar incertidumbre sobre el futuro de la legislación española de protección de datos personales.

Claro que el texto presenta importantes novedades, que han sido objeto de comentarios favorables, porque representan sin duda un fortalecimiento del sistema legal europeo de protección de datos personales, y cumplen con demandas que en materia de protección de datos habían sido reclamadas desde los más diversos sectores[43]; y así, según las enmiendas aprobadas (enmienda 27, Considerando 53), cualquier persona podrá solicitar la supresión de sus datos si no se cumplen las normas de la UE, los datos ya no son necesarios o la persona retira o no presta su consentimiento al almacenamiento de esa información[44]. En el caso de los datos procesados en internet, la empresa responsable tendrá que reenviar la solicitud de borrado a otras que hayan utilizado esa información. Este "derecho a la supresión" de los datos sustituirá al "derecho al olvido" propuesto por el ejecutivo de la UE. El derecho a solicitar la supresión de los datos quedará limitado cuando estos se hayan recabado con fines estadísticos, para la investigación histórica o científica, por motivos de salud pública o para ejercer la libertad de expresión.

Por otra parte, se prevé, con carácter general, que el interesado deba prestar su consentimiento expreso antes de que una empresa u organización pueda procesar sus datos personales. El consentimiento será entendido como una "manifestación libre, específica e informada de la voluntad del interesado, ya sea mediante una declaración o una clara acción afirmativa". Y así, conforme se señala en la Enmienda 12 del Parlamento, Considerando 33 del Reglamento, no constituye un fundamento jurídico válido cuando la persona no goza de verdadera libertad de elección y por tanto no está en condiciones de denegar o retirar su consentimiento sin sufrir perjuicio alguno. Así sucede especialmente cuando el responsable del tratamiento sea una autoridad pública que pueda imponer una obligación en virtud de sus poderes públicos al respecto y no se pueda considerar que el consentimiento se ha prestado libremente. Tanto es así, que la práctica habitual por la cual el interesado tenga que modificar la opción señalada por defecto para oponerse al tratamiento, como eliminar casillas ya marcadas, no constituye, en el marco de la futura norma europea, un consentimiento libre. Para poder acceder a un servicio no debe exigirse el consentimiento al tratamiento de datos personales adicionales que no sean necesarios para la

---

[42] Así lo ha entendido el Consejo de la Abogacía Europea, que reclama a las instituciones de la UE un único régimen de protección de datos a nivel global, en lugar de establecer dos regímenes distintos para los asuntos públicos y asuntos policiales respectivamente. Véase http://www.asociacion-eurojuris.es/publicaciones/derecho-de-las-nuevas-tecnologias-2/ (última consulta: 10/06/2014)

[43] Destaca la favorable acogida en el sector de marketing directo del denominado "sello europeo de protección de datos", que a juicio de los expertos generará mayor grado de confianza en los clientes, y la posibilidad de evitar las sanciones más graves por vulneración de las normas de protección de datos. Cfr. http://www.marketingpositivo.es/2014/04/sello-europeo-proteccion-datos.html (última consulta: 07/06/2014)

[44] Véase la SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala), de 13 de mayo de 2014. En http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=245907 (última consulta: 03/06/2014).

prestación de dicho servicio; se impiden así habituales prácticas como mantener marcada la casilla de "aceptar" en las políticas de privacidad.

Las nuevas Enmiendas también contemplan límites a una práctica conocida como "profiling", que consiste en la elaboración de perfiles mediante el procesado automático de los datos para analizar o prever el comportamiento de una persona, su situación económica, salud, preferencias, fiabilidad trabajo, su situación o localización. Este tipo de perfiles se utilizan, principalmente, para evaluar si una persona está en condiciones de devolver un crédito, o de desempeñar un determinado puesto laboral o profesional. En estos casos se establecen garantías legales específicas y se reconoce al interesado el derecho de información previo y la oposición al tratamiento de dicha información (art. 20).

VI. A MODO DE CONCLUSIÓN FINAL

Seguramente todos coincidiremos en señalar que la significativa evolución que se ha producido en el ejercicio de la abogacía en los últimos años no hubiera sido posible sin la incorporación de los avances de la sociedad de la información. Así, las comunicaciones personales, el tratamiento y consulta de la información, y también, cómo no, la gestión de propio despacho no han podido sustraerse a la realidad tecnológica, que ha facilitado y enriquecido la actividad profesional. Las bases de datos, el correo electrónico, el tratamiento informatizado de la información personal, la publicidad en páginas web corporativas, los blogs… y también los servicios de "cloud computing" han revolucionado el ejercicio de la profesión jurídica, y han destapado las numerosas dificultades e incertidumbres jurídicas a las que los despachos de abogados deben enfrentarse en su actividad profesional.

Una de las mayores dificultades es sin duda la exigencia legal que se desprende del tratamiento de la información personal en el ejercicio de la abogacía, y el obligado respeto a la normativa de protección de datos personales. En efecto, la normativa de protección de datos personales representa una ineludible obligación para quienes obtienen, tratan y manejan información personal, siempre que dicho tratamiento no se efectúe en el estricto ámbito doméstico; en consecuencia, quienes ejercen como abogados deben tener presente la LOPD y su normativa de desarrollo en el ejercicio profesional, y deben adoptar e implantar cuantas medidas y estándares de seguridad sean precisos para garantizar además de un satisfactorio servicio de asistencia legal, una correcta utilización y manejo de la información personal precisa para la prestación de dichos servicios. Corresponde a los despachos de abogados esforzarse en el cumplimiento de las normas de protección de datos personales, ante el imparable avance tecnológico, si bien cabe esperar entonces de las instituciones la adecuada asistencia y tutela en dicha labor; de suerte que a las dificultades propias del ejercicio de la abogacía no se unan las los inconvenientes y limitaciones que la aplicación de esta normativa puede ocasionar en el ejercicio diario de la actividad profesional. Por ello, merecen nuestra atención iniciativas como las de la AEPD que, en colaboración con el Consejo General de la Abogacía, prepara y publica Informes y Guías que facilitan la adecuación de los despachos de abogados a la nueva realidad tecnológica a la que deben enfrentarse estos profesionales en su día a día.

Por otra parte, a propósito del tratamiento de datos personales y la utilización del "cloud computing" en los despachos profesionales, no cabe duda que como, se asegura por los expertos, el futuro está en la "nube", y que debe trabajarse para lograr conciliar las innegables ventajas de este nuevo servicio con las exigencias legales de seguridad de la información. Y así, los despachos, como responsables del tratamiento de los datos de sus clientes, deben elegir un proveedor que cumpla las exigencias legales, con especial atención a la información sensible que manejan y su obligación de secreto profesional. Ciertamente, la posibilidad de acceder a toda la información desde cualquier lugar y en cualquier momento, puede ser clave para la gestión y agilidad de un despacho, pero, para ello, se precisa la certeza de que la información se almacena en un lugar seguro y que el secreto profesional queda salvaguardado. Por ello, ha de reconocerse que la

gestión de los despachos de abogados se puede volver mucho más eficiente gracias a la nube, con el consiguiente ahorro de recursos y tiempo.

En definitiva, quien ejerce la profesión jurídica como abogado debe tener siempre presente que el cumplimiento de la LOPD es inexcusable legalmente, y que del mismo no sólo depende evitar las elevadas sanciones previstas en las actuales normas de protección de datos personales (hasta 600.000 euros en las infracciones más graves), sino que el cumplimiento de la Ley se percibirá por los terceros como un signo de seguridad y confianza en los servicios prestados, y sin duda, contribuirá a mejorar y reforzar la imagen y credibilidad profesional.

VII. REFERENCIAS BIBLIOGRÁFICAS

Y. ADSUAR. "Cloud computing vs protección de datos de carácter personal", *Actualidad Jurídica Aranzadi,* núm. 846, 2012.

J. ALVAREZ HERNANDO,. "GUÍA PRÁCTICA SOBRE PROTECCIÓN DE DATOS. Cuestiones y Formularios". Lex Nova, Valladolid, 2011, pp- 377-ss.

J.A. ANDINO LÓPEZ, *Efectos de la vulneración del secreto profesional del abogado en el proceso civil.* Facultat de Dret. Universitat de Barcelona, Barcelona, 2013, pp. 103-107.

M.A. DAVARA RODRÍGUEZ, *Guía práctica de protección de datos para abogados*, Editorial DaFeMa, Madrid, 2004.

E. PÉREZ GÓMEZ, "¿Por qué proteger la información en los despachos de abogados?", *IURIS*, núm. 147, marzo de 2010.

E. PÉREZ GÓMEZ, "La protección de datos de carácter personal en un despacho de abogados", *Diario La Ley*, núm. 7524, Año XXXI, 9 de Dic. de 2010

B. LLORENTE GUILLÉN, "Análisis del deber de secreto de la Ley orgánica de protección de datos en relación con el secreto profesional de los abogados", *Anuario de la Facultad de Derecho. Universidad de Alcalá de Henares,* 2009, núm. 2, pp. 503-514.

R. MARTÍNEZ MARTÍNEZ, "El Real Decreto 1720/2007, de 21 De diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Aspectos clave", *Revista Jurídica de Castilla y León*, núm. 16, 2008, pp. 257-293.

R. MIRALLES, "*Cloud computing* y protección de datos", *Revista de Internet, Derecho y Política*, núm. 11, 2010, pp. 14-23.

J. R. MORALES, "Cloud computing: riesgos corporativos e implicaciones jurídicas". *Actualidad Jurídica Aranzadi*, núm. 863, 2013, pp-3-4.

V. REDING, "Protección de la privacidad en un mundo conectado. Un marco europeo de protección de datos para el siglo XXI", en J. PÉREZ y E. BADIA (coords), *El debate de la privacidad y seguridad en la red: regulación y mercados,* Ariel/Telefónica, Madrid, 2012, pp. XVII-XXV.

J. VERDAGUER LÓPEZ, "Tratamiento de datos personales en función del tipo de despachos", *Revista IURIS,* núm. 129, 2008, pp. 32-36.