La nueva regulación en protección de datos personales y su impacto en la actividad de los abogados

Javier Álvarez Hernando,
abogado y delegado de Protección de Datos

Se aproximan cambios importantes en materia de protección de datos, también para nuestra actividad profesional como abogados. En primer lugar, como norma estrella, se impone el Reglamento europeo 2016/979 (en adelante, RGPD), que será directamente aplicable desde el 25 de mayo de 2018, a lo que le seguirá la aprobación de una nueva Ley Orgánica de Protección de datos, que sustituirá a la actual LOPD (L.O. 15/1999).

Esta reforma va a exigir a los abogados mostrar cierta sensibilidad y concienciación en protección de datos. Un letrado en ejercicio está obligado a tener unas nociones básicas en esta materia, al igual que ocurre con otras ramas del derecho, que, si bien no imponen una especialización en un profesional, sí que se presupone que se debe disponer de una cierta cultura normativa en privacidad. Sobre todo, cuando la ciberseguridad y la digitalización de los despachos es una realidad creciente, impulsada en mayor o menor medida por un inseguro, atávico, "bug-eado"[1] y "glitch-eado"[2] sistema de comunicación electrónica bautizado como LexNet.

Cuando hablamos de protección de datos debemos partir por considerar que se trata de un derecho fundamental (distinto y diferenciado de la intimidad, del art. 18 CE) exclusivo de personas físicas, que busca proteger sus datos frente a intromisiones ilegítimas en la intimidad. El Tribunal Constitucional (STC 290/2000, de 30 de noviembre) configuró este derecho como fundamental, reconociendo el poder de disposición y control por parte de los interesados sobre sus propios datos.

Un "dato de carácter personal" es cualquier información concerniente a personas físicas identificadas o identificables. Y todos aquellos que traten datos personales, como hacemos los abogados en nuestra actividad, debemos cumplir con las previsiones que establece el RGPD.

El Reglamento europeo impone un cambio de paradigma, al introducir el llamado principio de responsabilidad activa o *accountability*, que impone al responsable, y al encargado del tratamiento, es decir al despacho o al abogado, estar en condiciones de demostrar que cumple con las previsiones normativas en materia de protección de datos.

> Esta reforma va a exigir a los abogados mostrar cierta sensibilidad y concienciación en protección de datos

En el RGPD, desde un punto de vista general, todo tratamiento de datos personales exige una base jurídica que lo legitime, (artículo 6 RGPD):

a) Consentimiento de afectado (que debe ser libre, explícito y específico para cada finalidad y que pueda ser revocado). Deja de ser válido el consentimiento tácito.

b) Existencia de una relación contractual (por ejemplo, a través de hojas de encargo).

c) Existencia de un interés legítimo prevalente del responsable o de terceros a los que se ceden o comunican los datos personales (artículo 6.1.f y Considerando 47 del RGPD).

d) Justificado en una necesidad vital del interesado.

e) Cuando resulte una obligación legal para el responsable del tratamiento.

f) Exista un interés público o se derive del ejercicio de poderes públicos.

¿Qué debe hacer un abogado para adaptar su actividad al RGPD?

1) Desaparece la obligación formal, hasta este momento, de notificar ficheros al Registro General de Protección de Datos.

2) Análisis de riesgos y medidas de seguridad adecuadas.

El despacho de abogados debe hacer un análisis de riesgos (artículo 32.1 RGPD) y determinar las medidas de seguridad adecuadas, pero NO debe realizar una evaluación de impacto, que se regula en el artículo 35 RGPD. Este análisis de riesgos debe hacerse desde una doble vertiente: 1) medidas de seguridad técnicas y organizativas (muy importantes); 2) riesgos para los derechos de las personas.

Deben implementarse medidas de seguridad (artículo 32.1 RGPD) atendiendo a los riesgos concretos que tengamos en los despachos, si bien el Reglamento muestra preferencia por medidas como el cifrado de los datos; medidas capaces de garantizar la confidencialidad, integridad, disponibilidad, resiliencia, restaurar

la disponibilidad y acceso a los datos; procesos de verificación, evaluación y valoración regulares. No se exige mantener un documento de seguridad, y la implantación de unas medidas concretas (por niveles) como ocurría hasta ahora, sino que se debe procurar tener unas medidas adecuadas al riesgo de nuestro despacho.

Resulta importante destacar que, con el Reglamento, el despacho o el abogado deben notificar las «quiebras de seguridad» que sufran (su concepto está en el artículo 4.12), en 72 horas tanto a la Agencia Española de Protección de Datos (en adelante, AEPD), como a los interesados, es decir, a los clientes (artículos 33 y 34 RGPD). En este sentido, tal y como ha manifestado la Directora de la AEPD no tienen intención de imponer sanciones a los despachos derivadas de esta notificación de quiebras de seguridad, salvo que aprecien cierta gravedad en la actuación del despacho.

3) Se exige al abogado mantener un registro de actividades de tratamiento. El contenido que debe tener este registro, que debe estar a disposición de la AEPD, se encuentra detallado en el artículo 30 RGPD.

4) Existe la obligación de dar cumplida respuesta a los derechos que ejerza el cliente, como son el de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad (estos dos últimos son derechos nuevos). Existe un procedimiento detallado para ello (artículos 15 a 22 RGPD), fijándose el plazo de 1 mes para su satisfacción o negativa por parte del despacho.

5) Deben adecuarse las clausulas informativas en protección de datos que se suelen incluir en las hojas de encargo profesionales. Ahora se exige informar de la base jurídica que legitima el tratamiento de datos y del plazo de conservación de los mismos. Si bien, esta información podrá realizarse "por capas" o niveles, se recomienda revisar el artículo 13 del RGPD para elaborar una nota legal adecuada.

   Se recomienda, por otro lado, que se dispongan de cláusulas informativas específicas del propio letrado, cuando actúa en turno de oficio, ya que las que disponen los modelos generales que suscribe el interesado únicamente incluyen referencias a la Comisión del Justicia Gratuita, y al Colegio de Abogados, siendo necesario que el propio abogado informe (y lo pueda acreditar) al ser éste un corresponsable del tratamiento de datos para la defensa del cliente.

6) No se requiere al despacho de abogados, por regla general, contar con un delegado de protección de datos, regulado en los artículos 37 a 39 RGPD.

Deben adecuarse las clausulas informativas en protección de datos que se suelen incluir en las hojas de encargo

7) Se promueve por el Reglamento, la adhesión (artículo 24.3 RGPD) a códigos de conducta (artículo 40 RGPD) o mecanismos de certificación (artículos 25.3 y 42 RGPD).

8) Se exigen medidas de Protección de datos "desde el diseño" (artículo 25.1 RGPD) y "por defecto" (artículo 25.2 RGPD). Es decir, se impone la obligación de establecer medidas técnicas y organizativas adecuadas desde la concepción del proyecto de un nuevo servicio del despacho. Estas medidas deben ser aplicadas, además, por defecto, empleando los datos personales estrictamente necesarios para cada fin específico.

9) En ocasiones el abogado actúa como encargado del tratamiento (por cuenta y bajo la dirección de un tercero responsable). Esta relación, en lo que respecta a protección de datos, debe constar en un contrato con un contenido específico que detallan los artículos 28 y 29 REPD.

¿Debemos los abogados recabar el consentimiento de nuestros clientes y de la contraparte para tratar sus datos?

En cuanto a los datos de nuestros clientes, la base jurídica legitimadora sería la relación contractual o precontractual y, en su caso, el consentimiento para tratar los datos, plasmado en una hoja de encargo. No se basaría en el interés legítimo prevalente. Si bien, en cualquier caso, se debe informar de lo previsto en los artículos 13 y 14 RGPD.

En lo que respecta los tratamientos de los datos de la contraparte, la AEPD mantiene un criterio claro, desde hace años: se produce una colisión de derechos fundamentales, a saber, el de tutela judicial efectiva y el de protección de datos, debiendo prevalecer, en este supuesto, el contemplado en el artículo 24 de la CE, es decir, la tutela judicial efectiva y el derecho de defensa. Y es que si los abogados solicitan el consentimiento a los afectados de contrario o les comunican determinada información que se pudiera disponer procedentes de los clientes, podrían perjudicar claramente a su derecho a obtener la tutela judicial efectiva. En este sentido, el artículo 14.5.b RGPD no exige dar esta información cuando imposibilite u obstaculice gravemente el logro del tratamiento. En cualquier caso, y si afectado (contrario) ejerce uno de sus derechos de acceso, oposición, etc., se impone la obligación al abogado, como responsable del tratamiento, de contestar en este sentido expuesto, denegando el ejercicio, dentro de los plazos legales y siguiendo el procedimiento indicado en los artículos 15 a 22 RGPD.

Finalmente, existen una serie de datos que son considerados como "categorías especiales" o especialmente protegidos, a saber: los que se refieran a la origen étnico o racial; opiniones políticas; convicciones religiosas o filosóficas; afiliación sindical; datos genéticos y biométricos; datos de salud; vida u orientación sexual (artículo 9 REPD). Pensemos, por ejemplo, en informes forenses; demandas laborales que se refieren a la afiliación sindical del demandante, etc. Pues bien, como regla general, se prohíbe su tratamiento salvo: "cuando el tratamiento es necesario para la formulación, ejercicio o defensa de reclamaciones ya sea por un procedimiento judicial, administrativo o extrajudicial (Considerando 52 y artículo 9.2 f RGPD). Es decir, un abogado tendrá legitimidad para tratar este tipo de datos personales, en el marco de su actividad profesional, y exclusivamente con esta finalidad.

Con todo lo dicho, y con la barrera de mayo de 2018, los abogados debemos comenzar a preocuparnos en adaptar nuestros despachos a las exigencias del Reglamento europeo, con el fin de evitar, o minimizar el riesgo, de la posible imposición de sanciones y riesgos reputacionales inherentes.

(1) Un "bug" es un error de software que desencadena un resultado indeseado.

(2) Un glitch, en el ámbito de la informática, es un error que afecta negativamente al rendimiento o estabilidad de un programa.