Wolters Kluwer
NOVEDAD
Test de la especialidad penal para la prueba de acceso a la abogacía
5% de dto. Envío gratis
MÁS INFORMACIÓN



Entrevista a José Luis Piñar, DPO del Consejo de la Abogacía

# “El 25 de mayo cualquier abogado deberá estar preparado para cumplir el RGPD y para demostrar que lo cumple”

9-4-2018 | Wolters Kluwer

Con el nuevo Reglamento se pasa de un modelo basado en el mero cumplimiento de los preceptos de la ley, a un modelo de responsabilidad proactiva, en el que no se trata sólo de cumplir con la norma sino de que cada despacho y cada abogado, sea capaz de identificar las medidas que tiene que adoptar para garantizar la protección de los derechos de los interesados en el seno de su organización y poder demostrar, además, que cumple con el Reglamento.

Carlos B. Fernández. La cuenta atrás hacia el 25 de mayo, momento en que el Reglamento General de Protección de Datos comenzará a ser aplicable, continúa implacable.

Uno de los sectores más afectados por ese hecho es el de la abogacía. Y ello por una doble razón: no solo porque por la naturaleza de sus actividades deberá ser especialmente escrupulosa en la adaptación a sus mandatos, sino también porque deberá ser capaz de ofrecer a sus clientes el asesoramiento adecuado que van a necesitar para cumplir adecuadamente la nueva normativa.

Como muestra de la importancia de este cambio normativo para la profesión, destaca el hecho de que en fechas recientes el Consejo General de la Abogacía Española designara un Delegado de Protección de Datos (o DPO, como es generalmente conocido por la abreviatura inglesa de Data Protection Officer).

El nombramiento ha recaído en José Luis Piñar Mañas, catedrático de Derecho Administrativo de la Universidad CEU San Pablo y abogado, cuyo currriculum le acredita como una de las figuras más relevantes en cuanto a protección de datos de nuestro país. Baste recordar que, además de autor de numerosas publicaciones sobre esta materia, ha sido Director de la Agencia Española de Protección de Datos y que preside la Sección de Derecho Público de la Comisión General de Codificación que elaboró el anteproyecto de ley orgánica de protección de datos.

DIARIO LA LEY ha tenido ocasión de conocer su opinión sobre el impacto que el RGPD va a tener en el trabajo de la abogacía, así como sobre las principales novedades que caracterizan a este Reglamento.

La principal conclusión que podemos extraer de sus palabras es que el Reglamento implanta un nuevo modelo de protección de datos que introduce un cambio radical en su planteamiento. Si en el modelo anterior la norma legal (Directiva 95/46/CE y LOPD) especificaban el alcance de las obligaciones de responsables y encargados de tratamiento, el RGPD establece un modelo basado de responsabilidad proactiva, en el que, a partir de una serie

de principios que en todo caso se van a tener que respetar, se permite que cada responsable, identifique y defina las medidas a adoptar para garantizar el respeto de los derechos de los interesados en el ámbito concreto de su organización, a la vez que se le exige que pueda demostrar la adecuación de dichas medidas para cumplir dichos fines.

Es decir, ya no se trata tanto de la mera aplicación de unas reglas y prohibiciones, sino de permitir a los responsables una mayor libertad en la organización de sus recursos para cumplir con las exigencias de la norma, a cambio de una mayor responsabilidad de dichos responsables y encargados en caso de incumplimiento.

A la vez, los abogados van a contar con una nueva oportunidad de crecimiento profesional, pues por su especial formación, se encuentran particularmente cualificados para asesorar a empresas y profesionales en el cumplimiento de la nueva normativa, en una tarea en la que la colaboración con los técnicos va a resultar también imprescindible.

DIARIO LA LEY. EL PRÓXIMO 25 DE MAYO COMIENZA A SER APLICABLE EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS ¿QUÉ EFECTOS VA A TENER ESTA NORMA SOBRE LOS ABOGADOS?

José Luis Piñar: Efectivamente, el próximo 25 de mayo comenzará a ser plenamente aplicable el nuevo Reglamento General de Protección de Datos. Esto significa que, en principio, ese mismo día cualquier despacho de abogados, cualquier abogado, debería de estar ya preparado para cumplir el Reglamento.

Para los despachos de abogados esta norma va a suponer un cambio sustancial porque cambia el modelo mismo de protección de datos. De un modelo basado en el cumplimiento de los preceptos de la ley, hasta ahora la Directiva de 1996 y la Ley de 1999, se pasa a un modelo de responsabilidad proactiva, en el que no se trata sólo de cumplir con la norma sino de que cada responsable, cada despacho de abogados, cada abogado, sean capaces de identificar las medidas que tienen que adoptar para garantizar la protección de los derechos de los interesados y poder demostrar que cumplen con el Reglamento.

(/Content/Inicio.aspx)

Esto es un cambio radical de planteamiento, de sistema y de modelo porque implica asumir la responsabilidad de adoptar las medidas que cada responsable considere adecuadas, en función de su situación, para garantizar el pleno respeto a la protección de datos o, lo que es lo mismo, de garantizar el tratamiento legítimo de los datos personales que estén llevando a cabo.

Esto va a implicar conocer perfectamente el Reglamento, que es de directa aplicación y no necesita de trasposición, sino a lo sumo de adaptación a través de la Ley Orgánica que se está tramitando ahora en el Congreso.

DLL: ¿QUÉ ASPECTOS DE LA ACTIVIDAD DE LOS ABOGADOS SE VAN A VER MÁS AFECTADOS POR EL REGLAMENTO?

JLP: El RGPD va a afectar a los abogados y a los despachos de abogados en un doble sentido. Por un lado, en cuanto que ellos mismos aunque algunos no lo sepan, son responsables de los ficheros y de sus tratamientos y por ello tienen que aplicar el Reglamento en su actividad.

Esto supone, por un lado, que tienen que revisar los tratamientos que estén llevando a cabo y los contratos que en su caso hayan firmado con encargados del tratamiento, porque los abogados tratamos datos por cuenta de nuestros clientes y eso en ciertos casos implica una relación responsable-encargado que conlleva la necesidad de suscribir un contrato cuyas cláusulas se deben revisar.

Y lo mismo deben hacer con las cláusulas informativas que utilizan con sus clientes y, en particular, con los protocolos para atender los derechos de los interesados, tradicionalmente conocidos como ARCO - acceso, rectificación, cancelación y oposición-, a los que ahora habrá que añadir también el de portabilidad.

Pero, además, para los abogados y despachos de abogados el RGPD va a significar una enorme oportunidad de poder prestar nuevos servicios a sus clientes, tanto a los que ya están asesorando como a otros nuevos.

Se trata de una norma peculiar y compleja para cuyo cumplimiento por muchos empresarios y profesionales va a resultar fundamental el asesoramiento de un abogado experto en esta materia. Por tanto, dado que los abogados están en muy buena disposición de poder prestar ese servicio que necesitan sus clientes, creo que se presenta una oportunidad de negocio por la prestación de nuevos servicios profesionales de asesoramiento, consultoría, etc.

DLL: LA PROTECCIÓN DE DATOS PERSONALES ESTÁ MUY CONDICIONADA POR MUCHOS FACTORES TECNOLÓGICOS ¿CÓMO CREE QUE PUEDE AFECTAR ESTE HECHO AL TRABAJO DE LOS ABOGADOS EN ESTA MATERIA?

JLL: Yo creo que los abogados, ahora más que nunca, deben ir muy de la mano de técnicos. ¿Por qué? Porque no sólo se va a exigir a los responsables, a los abogados, a los despachos y a sus clientes adaptar el tratamiento de datos a la norma, sino también a las medidas de seguridad necesarias.

Y estas medidas de seguridad ya no se plantean desde el cumplimiento estricto de los preceptos que las regulan en el Real Decreto 1720/2007, sino en función de la situación real de riesgo para la protección de datos de cada tratamiento que lleve a cabo cada responsable. Y esto implica ir muy de la mano de técnicos.

> En general los abogados van a necesitar conocimientos o apoyo técnico para asesorar en protección de datos

Por tanto, va a ser muy difícil, en mi opinión, que un abogado preste un servicio completo de asesoramiento y consultoría a un cliente en materia de protección de datos si no tiene conocimientos técnicos o puede contar con el apoyo de un técnico que complete el servicio que presta a sus clientes.

(http://www.facebook.com/sharer.php?u=http://...+preparado+para+cumplir+el+RGPD+y+para+demostrar+que+lo+cumple&t=...)

DLL: ¿EN QUÉ CASO RECOMENDARÍA A LOS DESPACHOS DE ABOGADOS DESIGNAR UN DELEGADO DE PROTECCIÓN DE DATOS (DPO)?

JLL: Los despachos de abogados no es que puedan sino que en muchos casos van a tener que designar un DPO.

Para ello hay que distinguir entre el abogado individual o el despacho de abogados. El Grupo de Trabajo del artículo 29 [Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado por la Directiva 95/46/CE] ha indicado que es comprensible que a aquellos profesionales que ejercen individualmente su actividad –un médico, un abogado-, no se les exija contar con un DPO. Pero los despachos de abogados, en la medida que se encuentren en alguna de las situaciones previstas en el Reglamento General de Protección de Datos, es decir y fundamentalmente, que traten a gran escala categorías especiales de datos o datos de infracciones y sanciones, lo cual es muy habitual deben nombrar un DPO.

> Los despachos que traten a gran escala categorías especiales de datos o datos sobre infracciones y sanciones de sus clientes, deberán nombrar un DPO

Esto va a afectar a muchos grandes despachos y en particular a aquellos que se dediquen a ámbitos o materias relacionados con el Derecho penal o el Derecho sancionador, porque van a tratar necesariamente tratos de infracciones penales o de sanciones administrativas.

DLL: USTED HA SIDO DESIGNADO RECIENTE DPO DEL CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA ¿QUÉ OBJETIVOS SE HA FIJADO PARA ESTA ETAPA TAN IMPORTANTE PARA LA PROTECCIÓN DE DATOS?

JLL: El primero y más importantes es asesorar al Consejo como DPO con las funciones que recoge el Reglamento, de información, asesoramiento, consulta, interlocución con la Agencia de Protección de Datos, etc.

En este sentido el objetivo es que el Consejo adapte todos sus tratamientos al RGPD y para ello ya se están revisando los tratamientos de datos que se realizan, para ver en qué casos debe elaborarse o no una evaluación de impacto de la protección de datos. Igualmente se están revisando los contratos responsable-encargado y las cláusulas informativas que se utilizan con los titulares de los datos.

Pero hay también otro objetivo muy importante, y es que el Consejo quiere ser referente nacional e internacional en materia de protección de datos para la profesión, también en Europa y en Iberoamérica, con la idea de que la abogacía tiene ante sí una gran oportunidad pero también un gran reto que debe afrontar. Para ello el Consejo se ofrece a colaborar en la medida en que sea necesario con la Agencia de Protección de Datos para difundir, apoyar, promover la cultura de la protección de datos en la abogacía.

En tercer lugar el Consejo, pretende conseguir una homogenización de los criterios en relación con los tratamientos de datos en el ámbito de la abogacía.

> Los Consejos y Colegios profesionales van a ser muy importantes para conseguir una aplicación homogénea del RGPD en sus sectores de actividad

Y es que, como la directora de la Agencia ha señalado con buen criterio, las corporaciones de derecho público como los Consejos y Colegios profesionales, no sólo de la abogacía aunque a este colectivo le afecte en particular, están llamados a tener un protagonismo muy importante para conseguir esa homogenización en la aplicación del Reglamento en sectores concretos.

Eso es lo que quiere hacer el Consejo en el ámbito de la abogacía y para ello está dispuesto a colaborar y ayudar a todos los Colegios que así lo soliciten. Por ejemplo, dado que el RGPD permite que haya un DPO para varias entidades públicas, podría plantearse la posibilidad de que el Consejo preste los servicios derivados de la protección de datos a aquellos Colegios que así lo solicitasen porque carezcan de medios para afrontar esas tareas o porque lo consideren oportuno.

DLL: ¿ALCANZARÍAN ESTOS SERVICIOS A LOS PROPIOS COLEGIADOS? ¿PODRÍA DESIGNAR EL CONSEJO UN DPO PARA LOS COLEGIADOS?

JLP: Creo que eso sería un poco difícil, porque mientras que la mayoría de tratamientos que realizan los Colegios sobre los datos, tanto privados como públicos que gestionan son muy semejantes y homogéneos, las circunstancias en las que trabajan los abogados pueden ser muy diferentes entre sí.

Por eso en mi opinión es más viable organizar una prestación de servicios homogéneos de DPO a los Colegios.

Creo que es importante destacar a este respecto que tanto el RGPD como el proyecto de la Ley Orgánica de Protección de Datos que se encuentra en tramitación en el Congreso, establecen que los Consejos y los Colegios profesionales están obligados a tener un DPO en relación con los tratamientos que tengan que ver con el ejercicio de sus funciones públicas, pero no en otros casos. Para las actividades de carácter privado pueden designar también un DPO, pero este sería de carácter voluntario. Sin embargo, en mi opinión, lo lógico es que el DPO se ocupe de todos los tratamientos que se lleven a cabo.

No quiero dejar de señalar a este respecto que la presidenta del Consejo, Victoria Ortega, tuvo muy claro desde el principio que era imprescindible que el Consejo contase con un Delegado de protección de datos y que por ello apoya totalmente la labor del Delegado. Además, también está impulsando que el Consejo se posicione en el ámbito europeo y en el ámbito iberoamericano, para que pueda ser un referente en materia de protección de datos no sólo a nivel nacional sino también en Europa y en Iberoamérica.

DLL: UNA DE LAS CRÍTICAS MÁS REPETIDAS QUE HA RECIBIDO EL RGPD ES QUE, POR LA CANTIDAD DE REQUISITOS Y CONDICIONANTES QUE INTRODUCE, ES UN NORMA DE DIFÍCIL CUMPLIMIENTO ¿COMPARTE ESA OPINIÓN? ¿ESTAMOS ANTE UN TEXTO QUE NO SE PUEDE CUMPLIR?

JLP: Sobre este tema puedo decir que yo mismo he ido cambiando de opinión a medida que he ido analizando, descubriendo y conociendo el Reglamento.

Una primera impresión es que se trata de una norma muy difícil de cumplir, pero a medida que se va conociendo su filosofía y alcance se cae en la cuenta de que lo que hace es fijar un marco normativo que permite a los responsables adaptar su realidad a la protección de datos.

> Los principios de responsabilidad proactiva y de privacidad desde el diseño permiten al responsable que adopte las medidas oportunas para la protección de datos a su caso concreto

Cuando se habla de la responsabilidad proactiva, de la privacidad desde el diseño y de la privacidad por defecto, lo que realmente se está diciendo al responsable es que en función de su situación concreta, tome las medidas oportunas para respetar la protección de datos.

Es verdad que con esta norma el consentimiento pasa a ser explícito en lugar de tácito, que las obligaciones de información se incrementan; que ya no hay que registrar ficheros pero que hay que llevar un registro de actividades del tratamiento; que aparecen nuevos derechos de los interesados, como el derecho a la portabilidad, y otras cuestiones concretas que hay que tener en cuenta y que pueden ser complejas. Pero también es verdad que un responsable puede analizar con mucha más precisión su situación concreta real y tomar las medidas que encajen en esa situación real para adaptarse al Reglamento.

Dicho esto, es cierto que para las pequeñas y medianas empresas va a ser más complicado cumplir con el Reglamento, porque el responsable de una entidad de cierto tamaño dispone de unos medios para definir los riesgos y para tomar medidas de las que puede carecer el responsable de una empresa pequeña o mediana, y esto quizá si que puede encarecer y complicar el cumplimiento.

Por eso es importantísimo el papel de las autoridades de protección de datos, como las Agencias, el grupo de trabajo del artículo 29 y del futuro Comité europeo de Protección de Datos, porque van a tener que jugar un papel no sólo de supervisión, control, regulación y sanción sino también de ayuda a las PYMES, fomentando y generando una cultura de protección de dato. En este sentido tanto el grupo de trabajo del artículo 29 como las Agencias de Protección de datos están elaborando directrices y guías para facilitar el cumplimiento. Esto es muy importante porque dada esa libertad de que va a gozar cada responsable para definir y establecer las medidas que considere adecuadas y pertinentes a su caso concreto, con esos documentos las Agencias facilitan bastante el cumplimiento normativo.

DLL: OTRO DE LOS ASPECTOS QUE HA SUSCITADO DUDAS SOBRE ESA DIFICULTAD DE CUMPLIMIENTO ES LA EXIGENCIA DEL CONSENTIMIENTO COMO UNO DE LOS PRINCIPIOS LEGITIMADORES DEL TRATAMIENTO ¿CREE QUE ELLO VA A CONVERTIR AL INTERÉS LEGÍTIMO EN LA PIEDRA ANGULAR REAL DEL TRATAMIENTO DE DATOS?

JLP: En efecto, el Reglamento opta por la exigencia de un consentimiento explícito que excluye la validez del consentimiento tácito y requiere una acción positiva para entender que aquél se ha otorgado. Y esto da pie a que otros títulos habilitantes, y entre ellos el interés legítimo, adquieran un protagonismo que quizá hasta ahora no tenía.

Sin embargo hay que recordar que el interés legítimo como principio legitimador del tratamiento ya existía en el derecho a la protección de datos desde la Directiva 95/46, no es algo nuevo. Lo que sucede es que en España era un criterio casi inédito porque los supuestos de intereses legítimos se reconducían a supuestos que estaban previstos en la ley.

Por otra parte, tras el criterio establecido por el Tribunal de Justicia de la Unión Europea en su sentencia ASNEF y FECEMD [de 24 de noviembre de 2011, asuntos acumulados C-468/10 y C-469/10], el legislador no puede definir cuáles son los supuestos de intereses legítimos que legitimen el tratamiento por parte del responsable, sino que tiene que ser el propio responsable quien lo haga.

Sin embargo, el legislador europeo quiso que el Reglamento sea una norma de unificación; por ello, si se permitiese que cada Estado fijase supuestos específicos que definiesen el interés legítimo que alteren el régimen común, se acabaría con la pretendida unificación del régimen de protección de datos.

Desaparecido el título habilitante consistente en que el tratamiento es válido si así está previsto por una ley, quedan como títulos habilitantes el consentimiento del afectado, que el tratamiento sea necesario para ejecutar un contrato en el que el interesado es parte, o para el cumplimiento de una obligación legal o que sea necesario para el cumplimiento de una misión realizada en interés público, y, por último, que sea necesario para la satisfacción de un interés legítimo del responsable del tratamiento.

> El interés legítimo se va a utilizar más que antes como título habilitante del tratamiento, va a asumir muchos tratamientos hasta ahora basados en el consentimiento tácito

Por ello, si no como piedra angular, el interés legítimo sí que va a ser un título habilitante que se va a utilizar mucho más de lo que hasta ahora se venía utilizando. Y quizás se van a tener que reconducir al tratamiento basado en el interés legítimo tratamientos que hasta ahora se amparaban en consentimientos tácitos o en lo que una ley establecía; por ejemplo el tratamiento para fines de solvencia patrimonial y crédito, hasta ahora contemplados en el artículo 29 de la LOPD, podrán ser considerados lícitos en base al interés legítimo del responsable, algo que el proyecto de Ley Orgánica así considera.

Con todo, hay que tener en cuenta que el interés legítimo no opera con la extensión que muchos pretenden porque, por ejemplo, no juega en relación con los tratamientos de categorías especiales de datos (los ahora llamados datos especialmente protegidos) ni en el ámbito de los poderes públicos. Las autoridades y los organismos públicos no pueden invocar un interés legítimo porque el título que les habilita es el ejercicio de un poder público o de un interés público. Por tanto, el interés legítimo está más limitado de lo que se ha dicho, porque el propio Reglamento lo ha fijado así.

DLL: UN ASPECTO RELEVANTE DE ESTE REGLAMENTO ES SU ÁMBITO DE APLICACIÓN TERRITORIAL, QUE LO HACE APLICABLE A AQUELLO TRATAMIENTO DE DATOS PERSONALES DE INTERESADOS QUE RESIDAN EN LA UNIÓN, POR PARTE DE UN RESPONSABLE O ENCARGADO NO ESTABLECIDO EN LA UNIÓN. ES DECIR, QUE ALCANZA A DESPACHOS SITUADOS, POR EJEMPLO, EN LATINOAMÉRICA O EN LOS ESTADOS UNIDOS, RESPECTO DE SUS CLIENTES EN LA UNIÓN.

JLP: En efecto. Si un despacho que no tiene oficina en la Unión Europea, ofrece, por ejemplo, servicios de asesoramiento a un residente en la Unión, estará sujeto al Reglamento y tendrían que cumplir con sus disposiciones.

> El RGPD va a ser la norma de referencia mundial en materia de protección de datos, porque cualquier empresa que ofrezca servicios en la UE va a tener que adaptarse a él

Esto permite afirmar que el Reglamento está llamado a ser la norma de referencia a nivel mundial en materia de protección de datos, porque no ya sólo las grandes compañías multinacionales que todos tenemos en la cabeza, sino cualquier compañía grande, pequeña o mediana que ofrezca productos y servicios a quien esté en la Unión europea va a tener que adaptarse a sus mandatos.

Pensemos en una agencia de viajes que ofrezca sus servicios desde fuera de la Unión, a través de internet; o en una compañía aérea que no tenga sede en la Unión Europea y ofrezca vuelos internacionales desde una ciudad a otra de Asia o desde una ciudad a otra de América, cuyos pasajes se adquieren desde la Unión. En estos casos esas entidades también tienen que someterse al Reglamento.

DLL: UNA DUDA QUE MUCHOS TIENEN EN ESTO MOMENTOS: LLEGA EL 25 DE MAYO Y NO HAY LEY ORGÁNICA DE PROTECCIÓN DE DATOS ¿QUÉ SITUACIÓN SE PRODUCE?

JLP: En ese caso se produciría una situación muy interesante. Por un lado, porque, llegada esa fecha, el Reglamento será de directa aplicación en todos sus términos y a todos sus destinatarios, sin necesidad de ninguna ley de trasposición. Y por otra parte porque esta norma comunitaria no deroga por sí misma a normas nacionales, sino que las desplaza.

Aunque no haya LOPD en mayo, no habrá vacío normativo, el RGPD será de directa aplicación en todos sus términos, desplazando a las normas nacionales

De modo que el 25 de mayo no se va a producir una situación de vacío normativo. La Directiva 95/46 quedará derogada, eso es claro, y las normas nacionales quedarán desplazadas en lo que se opongan al Reglamento.

Pero subrayo que en lo que se opongan, no en su totalidad, y pongo dos ejemplos: el Reglamento dice que ya no hay que inscribir los ficheros en la Agencia, de esta manera la regulación que se refiere a la inscripción de ficheros en la LOPD queda desplazada, pues ya no hay que inscribir los ficheros. Por otro lado, el Reglamento deja en manos de cada Estado determinar si se puede imponer multas económicas no a la administración pública; la LOPD opta por que no cabe imponer multa a las administraciones públicas, lo no queda desplazado porque es una opción legítima de los Estados miembros que encaja con el Reglamento.

Otro ejemplo: la normativa vigente se refiera sólo a los derechos de acceso, rectificación, cancelación y oposición. Pues bien, esta disposición queda desplazada porque ahora también se reconoce el derecho de portabilidad, o el derecho de supresión, entendido también como el derecho al olvido; igualmente los sistemas de información a los titulares de los datos regulados actualmente, quedan desplazados porque ahora hay mayores niveles de información y transparencia; en cuanto al régimen aplicable a las medidas de seguridad según el Real Decreto 1720/2007, quedará desplazado en la medida en que se consideren per se suficiente las medidas de seguridad que establece ese Real Decreto. Ahora, cada responsable tendrá que valorar si esas medidas de seguridad son o no adecuadas.

Y finalmente, también queda desplazada la regulación del citado Reglamento aprobado por Real Decreto de 2007 cuando prevé que cada dos años habrá que elaborar una auditoría del tratamiento de datos especialmente protegidos. Ahora ya no le vale a un responsable con decir que cumple con pasar una auditoría cada dos años, porque según la actividad que realice y el riesgo que el tratamiento de datos implique para los afectados, puede que en realidad tenga que pasarla cada año o cada seis meses o cada tres años (eso ya dependerá del responsable, pues el Reglamento de 2007 en este sentido pasaría a ser tan sólo marco de referencia).

DLL: ¿QUÉ CONSECUENCIAS PREVÉ QUE PODRÍA TENER LA AUSENCIA DE ESA LOPD EN CUANTO A LOS PROCEDIMIENTOS Y A LAS SANCIONES POR PROTECCIÓN DE DATOS?

JLP: En cuanto a los procedimientos hay que destacar que la Ley 39/2015, reguladora del procedimiento administrativo, no encaja bien con los procedimientos trasnacionales que regula el RGPD. Los procedimientos en los que entran en juego otras autoridades extranjeras no están previstos en la ley 39/2015.

En estos casos, a falta de una LOPD, la Agencia va a tener que adaptar sus procedimientos y analizar muy detenidamente cómo pueden regularse o definirse los procedimientos que va a llevar a cabo.

DLL: EL PROYECTO DE LEY ORGÁNICA EN TRAMITACIÓN HA APOSTADO POR UNA TIPIFICACIÓN MUCHO MÁS PRECISA DE LAS CONDUCTAS SANCIONABLES QUE LA ESTABLECIDA EN EL REGLAMENTO ¿CREE QUE ESTA TIPIFICACIÓN SATISFACE LAS EXIGENCIAS DE SEGURIDAD JURÍDICA PREVISTAS EN NUESTRO ORDENAMIENTO?

JLP: En efecto, este fue uno de los temas que nos planteamos en la Comisión de Codificación al elaborar el anteproyecto de la Ley.

El artículo 83 del Reglamento estable los criterios generales para la aplicación de sanciones, pero esos criterios generales se tienen que concretar a partir de unos criterios que aporta el propio Reglamento al distinguir entre conductas que pueden dar lugar a una sanción de hasta 10 millones de euros o el dos por ciento del volumen de negocio total anual global, y conductas que pueden dar lugar a sanciones de hasta 20 millones de euros o el cuatro por ciento de ese mismo volumen de negocio.

Y esos son los criterios que en principio deberán tenerse en cuenta, porque lo cierto es que la tipificación de la actual LOPD no encaja fácilmente con el Reglamento General de Protección de Datos.

Con el RGPD las autoridades de protección de datos van a tener mayor margen para apreciar si una conducta es sancionable, pero también van a tener que motivarlo más

La carencia de una Ley adaptada al Reglamento va a generar la necesidad de que la Agencia interprete las conductas que puedan ser consideradas como infractoras. Y en este sentido es muy importante señalar que a partir del 25 de mayo, todas las autoridades de protección de datos, no sólo la Agencia española sino todas las autoridades de protección de datos , van a tener un mayor margen de apreciación a la hora de determinar si una conducta es o no constitutiva de infracción.

Como antes decíamos, el modelo de protección de datos es ahora distinto. Y esto va a obligar a las autoridades a motivar mucho más las resoluciones que adopten. Pongo un ejemplo: en la actualidad, si la Agencia lleva a cabo una inspección en la que se aprecia que un responsable que debería haber llevado a cabo una auditoría cada dos años no lo ha hecho, concluirá que esa conducta implica imponer una sanción. Pero con el Reglamento Europeo la Agencia va a tener que determinar si el plazo por el que ha optado un responsable es el adecuado o no. Y si la Agencia considera que no es adecuado va a tener que motivar en su resolución por qué lo entiende así.

O por explicarlo de otro modo más burdo pero muy simple: en materia de tráfico circular a 121 km/hora en un tramo limitado a 120, supone una infracción a la que cabe imponer una multa sin necesidad de mayor motivación que la prueba del hecho. Pero a partir de ahora, será posible imponer una multa aunque se circule a 110 km/hora Si no se es capaz de justificar es velocidad. Es decir, el nuevo procedimiento sancionador ya no es tan reglado o tan mecánico. Lo que por otra parte implica que las Autoridades van a verse obligadas a motivar mucho más sus resoluciones.

DLL: SE TRATA DE SEGUIR UN MODELO DE RESPONSABILIDAD ANGLOSAJÓN …

JLL: Efectivamente, pasamos a un modelo anglosajón que, como se ha dicho, considera a los ciudadanos como mayores de edad. Los responsables y encargados deberán adoptar las medidas adecuadas para garantiza y poder demostrar el cumplimiento de la norma. Las Autoridades de control no van a estar encima de aquéllos, pero pueden y deben llevar a cabo una función de supervisión. De modo que si consideran que un responsable ha llevado a cabo una conducta que en principio puede ser infractora, y no demuestra que lo que ha hecho es adecuado y pertinente, podrán imponerle una sanción. A partir del 25 de mayo no va a ser tanto una cuestión de aplicación de reglas y prohibiciones sino de mayor libertad, pero también de mayor responsabilidad, por parte de los responsables y encargados.

_____

Para saber más:

Wolters Kluwer pone a su disposición el más completo conjunto de herramientas, cursos de formación y materiales de trabajo para facilitarle el cumplimiento del RGPD

- Complylaw Privacidad
- El nuevo marco regulatorio derivado del Reglamento europeo de protección de datos
- Aplicación práctica de la protección de datos en las relaciones laborales
- Reglamento Europeo de Protección de Datos
- Programa Ejecutivo Data Protection Officer (DPO)
- Aplicación práctica y adaptación de la protección de datos en el ámbito local

Opinar (0)