El nuevo Reglamento General de Protección de Datos

ÁLVARO ABÁIGAR DOMÍNGUEZ
ABOGADO / ASOCIADO EN ARPA ABOGADOS CONSULTORES
DIRECTOR DEL DEPARTAMENTO DE NTIC & IP

El próximo 25 de mayo de 2018 será de aplicación el Reglamento General de Protección de Datos, que tiene como objetivo principal actualizar el marco normativo en la materia, ya que la Directiva del año 95 venía siendo insuficiente en muchos puntos. Asimismo, pretende lograr una mayor uniformidad en su aplicación en los diferentes países de la Unión Europea (UE). Este último objetivo se va a ver facilitado por la aplicación directa del Reglamento sin necesidad de que los Estados miembros desarrollen ningún tipo de legislación. En el presente artículo, vamos a tratar algunos de los muchos cambios que trae el nuevo Reglamento.

ÁMBITO TERRITORIAL

La novedad más significativa en materia territorial es dejar meridianamente claro que esta normativa será de aplicación a cualquier tratamiento de datos de interesados que residan en la UE cuando las actividades de tratamiento estén relacionadas con la oferta a estos interesados de bienes y servicios o al control de su comportamiento. Por tanto, una plataforma tecnológica de cualquier parte del mundo deberá someterse a esta normativa de protección de datos si efectivamente dirige sus servicios a residentes de la UE.

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

El concepto de *«privacidad desde el diseño»* se refiere a la necesidad de establecer una metodología de desarrollo de productos y servicios que traten datos de carácter personal que tenga en cuenta la normativa sobre protección de datos lo antes posible en el proceso de desarrollo. Sólo de esa manera se minimiza la posibilidad de que lleguen al mercado productos contrarios a la normativa. Por ese motivo, si no lo hemos hecho todavía, debemos incorporar en nuestros procesos de concepción y desarrollo de productos y servicios la visión de protección de datos.

Y *«la privacidad por defecto»* quiere decir que solo sean objeto de tratamiento aquellos datos personales que sean realmente necesarios para cada uno de los fines específicos del proceso de que se trate. O lo que es lo mismo: solo debemos tratar aquellos datos que estrictamente necesitemos y debemos hacerlo de una manera respetuosa con el derecho a la protección de datos. Esto tiene un impacto directo en la cantidad de datos personales recogidos, en la extensión de su tratamiento, en su plazo de conservación y en su accesibilidad.

OBTENCIÓN DEL CONSENTIMIENTO

El nuevo reglamento introduce nuevas exigencias y limitaciones en la obtención del consentimiento del interesado. La novedad más significativa es que deja de ser válida la obtención del consentimiento de manera tácita. A partir del 25 de mayo será necesario que el consentimiento se otorgue mediante un *«acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal»*. A estos efectos se recuerda en el Reglamento que *«el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento»*.

Asimismo, hay mayores exigencias de información, claridad y transparencia en el proceso de obtención del consentimiento. Por ejemplo, deberemos informar sobre el plazo de conservación de los datos.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Una de las primeras cuestiones a abordar por las organizaciones que deseen cumplir la nueva normativa de protección de datos, es elaborar el denominado *«Registro de las Actividades de Tratamiento»*. Se trata en esencia de identificar los tratamientos efectuados, asociándoles una determinada información, como por ejemplo los fines del tratamiento, las categorías de datos y, cuando sea posible, los plazos de supresión previstos o las medidas técnicas y organizativas de seguridad asociadas. Este registro viene a sustituir

a la obligación existente en algunos países (como el nuestro) de notificar, en nuestro caso a la Agencia Española de Protección de Datos, los ficheros existentes en cada organización. En efecto, a partir del 25 de mayo ya no será necesario *«dar de alta los ficheros»*.

Bajo nuestro punto de vista, el Registro de las Actividades de Tratamiento supone la piedra angular de cualquier proyecto de implantación en una organización: deben identificarse y estudiarse cada uno de los tratamientos que se llevan a cabo, analizando las circunstancias en que tienen lugar la entrada, tratamiento y en su caso salida de los datos. Sólo de esta manera se podrá determinar correctamente la base legal del tratamiento y, por ejemplo, solicitar el oportuno consentimiento a los interesados.

El Registro de Actividades de Tratamiento alcanza no sólo a las organizaciones que adopten un rol de responsables del tratamiento, sino también a aquellas que tratan datos por cuenta de terceros (los denominados *«encargados de tratamiento»).*

DELEGADO DE PROTECCIÓN DE DATOS

El Delegado de Protección de Datos (o *Data Protection Officer* en inglés) es sin duda una de las grandes novedades del nuevo Reglamento. Si bien en algún país europeo (por ejemplo, en Alemania) era una figura ya conocida y obligatoria, en el caso de España constituye una novedad, ya que la legislación actual no lo contemplaba.

En cualquier caso, hay que decir que no todos los responsables de ficheros y encargados tienen la obligación de nombrar a un Delegado de Protección de Datos. En efecto, el Reglamento indica que será obligatorio en los siguientes casos:

a) cuando el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
b) cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
c) cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

Como en ocasiones puede ser difícil determinar si nos hallamos o no ante un caso que exija nombrar a un delegado de Protección de Datos, el legislador español, en el proyecto de reforma de la Ley Orgánica de Protección de Datos (que al momento de redacción de este artículo está bajo trámite) ha considerado oportuno relacionar una serie de entidades que vendrían obligadas a su nombramiento: entidades aseguradoras y reaseguradoras; Universidades; establecimientos financieros; distribuidores y comercializadores de energía eléctrica; centros sanitarios legalmente obligados al mantenimiento de las historias clínicas, etc. En todo caso, debe señalarse que el nombramiento también puede ser voluntario (eso sí, quedando en consecuencia afecto al régimen legal).

Sobre las funciones del Delegado de Protección de Datos, debe destacarse la labor de informar y asesorar a las organizaciones sobre sus obligaciones en materia de protección de datos, así como las tareas de supervisión sobre el cumplimiento de la norma (que incluye la formación del personal y la realización de auditorías). También deberá implicarse en las evaluaciones de impacto, asesorando y supervisando su aplicación. Finalmente, merece la pena indicar su rol de cooperación y punto de contacto con las autoridades de control.

Con la implantación del nuevo registro de las actividades de tratamiento no será necesario dar de alta los ficheros en la AEPD

El Delegado de Protección de Datos podrá formar parte de la organización o desempeñar sus funciones en el marco de un contrato de servicios. Se permite que un grupo empresarial pueda nombrar un único Delegado de Protección de Datos siempre que sea fácilmente accesible desde cada establecimiento. En cualquier caso, sus funciones y cometidos no deberán dar lugar a conflicto de intereses.

En cuanto al perfil de la figura, se indica que deberá ser designado, atendiendo a sus cualidades profesionales y, entre otras, a sus conocimientos especializados del Derecho y la práctica en ma-

teria de protección de datos.

Una vez designado, deberá tener los recursos necesarios para el desempeño de sus funciones y el mantenimiento de sus conocimientos especializados. También la independencia es una característica definitoria de la figura: no podrá recibir ninguna instrucción sobre el desempeño de sus funciones, ni podrá ser destituido ni sancionado por desempeñar sus funciones.

El Delegado de Protección de Datos rendirá cuentas directamente al más alto nivel jerárquico de la organización.

MEDIDAS TÉCNICAS Y ORGANIZATIVAS

Hasta el momento, la regulación española venía determinando las medidas aplicar de acuerdo con el nivel de datos que tuviéramos. De esta manera había unas medidas de seguridad asociadas a cada uno de los tres niveles establecidos (básico, medio y alto). Todas las medidas debían recogerse en el denominado «*Documento de Seguridad*».

Ahora la aproximación es radicalmente diferente. La nueva normativa dispone que las medidas deberán determinarse «*teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas*». Cada organización deberá diseñar y elaborar un auténtico traje a medida en este punto, debiendo reflexionar sobre el nivel de seguridad que en cada caso proceda teniendo en cuenta los riesgos que presente cada tratamiento.

Sin duda un nuevo enfoque que, de un lado, viene a dar mayor flexibilidad a las organizaciones para centrarse en las medidas que efectivamente aporten valor desde el punto de vista de la seguridad, pero que sin duda también va a dificultar acreditar su cumplimiento.

VIOLACIONES DE SEGURIDAD

Con la entrada en aplicación del Reglamento General de Protección de Datos, las violaciones de seguridad deberán comunicarse sin dilación a la Agencia Española de Protección de Datos, o en su defecto, en un plazo no superior a 72 horas después de que haya tenido constancia del incidente. Incluso cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, la organización deberá comunicar al interesado sin dilación indebida el incidente.

A la vista de esta situación, las organizaciones deberán crear protocolos para la gestión de los incidentes de seguridad, ya que los plazos son ciertamente exiguos. Asimismo, al diseñar las medidas de seguridad, se deberá tener especial atención a este tipo de supuestos, ya que, si se han adoptado medidas de protección técnicas y organizativas apropiadas, como por ejemplo que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos (por ejemplo, mediante cifrado) no será necesario activar el protocolo de comunicación a la Agencia Española de Protección de Datos. En todo caso será necesario documentar este tipo de incidentes y, en su caso, las medidas correctivas adoptadas.

Finalmente, deberán tenerse en cuenta las repercusiones que pudieran generar este tipo de incidentes sobre la reputación de la organización.

EVALUACIONES DE IMPACTO RELATIVAS A LA PROTECCIÓN DE DATOS

Cuando sea probable que un tipo de tratamiento entrañe un alto riesgo, será necesario efectuar una evaluación del impacto, que tiene por objeto reflexionar sobre las cautelas a adoptar antes de que el tratamiento se produzca. Con ello, el legislador ha querido conseguir que, antes iniciar tratamientos de datos que pudieran comprometer el derecho a la protección de datos, se articulen las medidas oportunas o, en su caso, se desista de llevar a cabo dichos tratamientos.

Para la identificación de los tratamientos que requerirían de este tipo de evaluaciones, la normativa establece una serie de supuestos como, por ejemplo, los tratamientos a gran escala de las categorías especiales de datos. En cualquier caso, en ocasiones puede ser complicado determinar si un determinado tratamiento está exento o no de la obligación de efectuar un Informe de Impacto, se prevé la posibilidad de que se establezca y publique una lista de los tipos de operaciones de tratamiento que la requieran.

SANCIONES

En esta materia se ha aprovechado para homogeneizar el régimen sancionador en la UE, dado que había disparidad de aproximaciones en materia sancionadora. Es evidente que la protección efectiva de los datos personales exige que las infracciones se castiguen con sanciones equivalentes a la gravedad de las mismas y al daño causado. Aunque en el caso español la normativa de 1999 ya preveía sanciones económicas que podrían llegar hasta los 600.000 €, es evidente que en algunas situaciones esas sanciones podrían no llegar a cumplir su función de establecer un sistema sancionador efectivo, proporcionado y disuasorio.

Por estos motivos el Reglamento General de Protección de Datos ha endurecido notablemente las sanciones por incumplimiento, que pueden llegar a ser sancionados en los casos más graves con multas administrativas de hasta 20 millones de euros o una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Fijar un parámetro relativo vinculado a la facturación va a garantizar sin duda la efectividad de la disuasión pretendida. Paradójicamente, la UE, pese a contar con una de las regulaciones más intensas y rigurosas en materia de protección de datos, se había quedado atrás en materia de derecho sancionador para las grandes corporaciones. En los EE.UU., sin ir más lejos, se han conocido sanciones de varias decenas de millones de dólares (por ejemplo, Google fue sancionada en 2012 con 22,5 millones de dólares en el caso del seguimiento de los usuarios del navegador Safari).

El régimen sancionador tiene en cuenta la naturaleza, gravedad y duración de la infracción y su carácter intencional o no, así como las medidas tomadas para paliar los daños y perjuicios sufridos y la forma en que la autoridad de control haya tenido conocimiento de la infracción. Por ese motivo, las organizaciones debemos emplear nuestros mejores esfuerzos no sólo en diseñar y desplegar medidas orientadas al cumplimiento, sino también a la gestión de los incidentes que puedan darse, en especial a la forma y manera que podamos mitigar sus consecuencias.