Protección de Datos

Nuevo Reglamento de Protección de Datos

Enrique Peloche
Abogado
Nuevas Tecnologías

En enero del año pasado salió a la luz 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, esto es, el Reglamento General de Protección de Datos. Dicha propuesta se encuentra todavía en fase de tramitación y a día de hoy, ya ha recibido numerosas enmiendas que, sin duda, matizarán algunos de los puntos más conflictivos del texto normativo ya que afectan directamente a organizaciones con un peso específico dentro del espacio económico europeo.

El citado Reglamento, cuya entrada en vigor se prevé que será a comienzos del próximo año, derogará la Directiva 95/46/CE y por ende, la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la citada ley.

La propuesta normativa tiene un triple objetivo, por un lado, el fortalecimiento de los derechos de los afectados, por otro, hacer frente a los retos que plantean la globalización y las nuevas tecnologías en relación al tratamiento de datos y por último, conseguir la plena armonización de la normativa relativa al derecho fundamental a la protección de datos en la Unión Europea.

En relación a este último objetivo nos gustaría señalar que tiene una explicación lógica dado que la transposición de la Directiva vigente por parte de los Estados Miembros provocó una fragmentación normativa que dificultó, en buena medida, la libre circulación de datos personales dentro de la UE, creando con ello un marco de inseguridad jurídica que la presente propuesta pretende corregir. De hecho, la elección de la forma reglamentaria como medio para regular la protección de datos nos es baladí, hay que tener en cuenta que los reglamentos europeos son directamente aplicables en cada Estado Miembro.

Dicho lo anterior y volviendo al primero de los objetivos señalados, podemos observar que, tal y como avanzábamos en párrafos anteriores, los derechos de los titulares de datos se van a ver fortalecidos con las nuevas exigencias que impone el Reglamento, tanto a las organizaciones privadas como públicas que traten datos de carácter personal.

Para encarar este apartado limitaremos sus análisis a tres aspectos fundamentales que afectan directamente a dichas organizaciones en beneficio de los derechos e intereses de los titulares de datos.

En primer lugar hablaremos del concepto de protección de datos tanto desde el diseño como por defecto o "Privacy by desing / Privacy by default".

Lo que establece la propuesta, es que el responsable del tratamiento estará obligado a implementar en su organización, con carácter previo al tratamiento de datos, medidas y procedimientos técnicos y organizativos que garanticen que el tratamiento que realice o vaya a realizar sea conforme con las disposiciones del Reglamento y la protección de los derechos de los interesados. Así como, que dichos mecanismos deberán garantizar, por defecto, que sólo sean objeto de tratamiento, los datos personales necesarios para cada fin específico del tratamiento y que no se recojan ni conserven más allá del mínimo necesario para esos fines. Por último, deberán garantizar que, por defecto, el acceso a los datos tratados estará limitado a un número determinado de personas dentro de cada organización.

Esto, sin duda, supone una piedra de toque para que las empresas desarrolladoras de software, adapten los programas que desarrollen para sus clientes con el objetivo de que éstos puedan cumplir con las obligaciones anteriormente señaladas.

En segundo lugar, nos gustaría abordar otro de los aspectos que, a nuestro juicio, supondrán un salto cualitativo en relación a las medidas que las organizaciones deberán asumir respecto al tratamiento de determinados datos conforme al nuevo Reglamento. Nos referimos a las evaluaciones de impacto o análisis de riesgos relativos a la protección de datos o "Privacy Impact Assesment (PIAS)". Las PIAS serán necesarias cuando las operaciones de tratamiento entrañen riesgos específicos para los derechos y libertades de los interesados en razón de la naturaleza, alcance o finalidad con la que vayan a ser tratados los datos. Esta obligación recaerá tanto en el responsable como en el encargado que actúe por cuenta del primero.

El Reglamento señala, a título enunciativo pero no limitativo, algunas operaciones de tratamiento que entrañan los riesgos específicos, señalados de forma general en el párrafo anterior:

a. Cuando el tratamiento de datos tenga por objeto crear perfiles de personas destinados a analizar o predecir su situación económica, localización, estado de salud, preferencias, fiabilidad o comportamiento sobre la base de los cuales se produzcan efectos jurídicos que atañan o afecten significativamente a dichas personas.
b. Cuando la operación de tratamiento se realice a gran escala y tenga por objeto tratar datos sobre la vida sexual, la salud, la raza y el origen étnico de los titulares o esté destinada a la prestación de atención sanitaria, investigaciones epidemiológicas o estudios relativos a enfermedades mentales o infecciosas, en este caso, cuando los datos sean tratados con el fin de tomar medidas o decisiones sobre personas concretas.
c. Cuando se realicen operaciones de seguimiento de zonas de acceso público, es decir las relativas a la instalación de, por ejemplo, cámaras de video vigilancia a gran escala en la vía pública.
d. El tratamiento a gran escala de datos relativos a menores (en el nuevo Reglamento se establece que serán los menores de 13 años) o el tratamiento de datos genéticos o biométricos.
e. Además de otras operaciones de tratamiento que requieran la autorización previa de la autoridad de control (la Agencia Española de Protección de Datos en el caso de España).

En este sentido, el Reglamento establece los elementos mínimos que deberán incluir las PIAS, estos son, una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a los riesgos y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales.

Para terminar este apartado señalaremos que no deja de ser curioso lo que establece el siguiente punto del precepto analizado, y decimos curioso ya que su aplicación práctica resulta, cuanto menos, complicada. Lo que señala dicho punto es que los responsables del tratamiento recabarán la opinión de los interesados o sus representantes en relación con el tratamiento previsto. La verdad es que no me imagino el modo en que se pueda materializar esta consulta previa, ni qué criterios se emplearán para su valoración.

En tercer lugar, hablaremos de la figura del Delegado de Protección de Datos o "Data Privacy Officer" (DPO), cuya implementación en España supondrá que ya no será necesario notificar los ficheros ante la autoridad de control. Pues bien, según el Reglamento la obligación de designar un DPO recaerá tanto en los responsables como los encargados del tratamiento y siempre que se trate de organizaciones públicas, también cuando siendo organizaciones privadas tengan 250 o más empleados (aunque este punto es posible que cambie, ya que se está barajando la posibilidad de que la misma sea obligatoria para todo aquel responsable o encargado de tratamiento con ficheros que afecten a más de 500 titulares, lo cual ampliaría la obligación de designar a un DPO a todo tipo de organizaciones privadas) y, por último se señala que será obligatorio cuando las actividades principales del responsable o encargado de tratamiento consistan en operaciones de tratamiento que, por razón de su naturaleza, alcance y/o fines, requieran un seguimiento sistemático y periódico de los interesados.

En este sentido, cabe destacar las siguientes consideraciones:

a. Se permite que exista un único DPO para un grupo de empresas.
b. La designación del DPO será para un mandato mínimo de dos años y solo podrá ser destituido si deja de cumplir las condiciones requeridas para el ejercicio de sus funciones.
c. Los DPO podrán desempeñar sus tareas sobre la base de un contrato de servicios.
d. Los responsables o encargados de tratamiento deberán comunicar el nombre y los datos de contacto del DPO a la autoridad de control y al público.
e. El DPO actuará con total independencia sin que pueda recibir instrucciones en lo que respecta al desempeño de sus funciones, el cual informará directamente a la dirección de la organización.
f. Además el responsable o encargado de tratamiento facilitarán al DPO, el personal, los locales, los equipamientos, etc. que precise para el desempeño de sus funciones.

Entre las funciones que desempeñará el DPO destacaremos, las de informar y asesor a la organización en lo que respecta a sus obligaciones y documentar esta actividad, supervisar la implementación y aplicación de las políticas de privacidad (entre las que se encuentran las PIAS y la Privacy by Desing o by default en la organización), asignará responsabilidades dentro de la organización, se encargará de la formación del personal, de atender las solicitudes presentadas por los interesados en el ejercicio de sus derechos y realizar las auditorías correspondientes. Por último el DPO actuará como punto de contacto entre la autoridad de control (tanto la nacional como la comunitaria) y la organización.

En resumen podemos decir que el DPO será una figura clave dentro de las organizaciones ya que será el encargado de que en las mismas se cree una cultura de la privacidad acorde con el principio general que rige todo el Reglamento, esto es, el principio de control y rendición de cuentas o "Accountability", materializado a través de las PIAS, la Privacy by desing / by default y la cooperación con las autoridades de control que, además, está íntimamente unido a otro principio general que desarrolla el nuevo Reglamento como es el principio de transparencia cuyo objetivo es facilitar la comunicación entre las organizaciones y los interesados y las autoridades de control.

La actual propuesta de Reglamento supondrá, sin duda, un esfuerzo añadido para las organizaciones en el cumplimiento de sus obligaciones en relación al tratamiento de datos que realicen. Este último apartado es un buen ejemplo de lo que aquí decimos, ya que se verán en la obligación de contratar, al menos durante dos años, a un DPO, ya sea como empleado de la organización o como externo, para poder cumplir con las exigencias del nuevo Reglamento.

En resumen, con el presente artículo no pretendemos abarcar todas las novedades que trae consigo la propuesta del nuevo reglamento, que merecerían por su importancia un análisis más detallado debido a las consecuencias que conllevan, como las relativas a la seguridad de los datos (incluyendo la obligación de comunicar las brechas de seguridad a la autoridad de control y a los interesados) o los nuevos derechos de los interesados (como el conocido "Derecho al olvido", la portabilidad de datos, entre otros) o el nuevo régimen sancionador que se impondrá a los que infrinjan los preceptos del Reglamento (que incluye una sanciones que pueden resultar desmesuradas, si tenemos en cuenta que se podrán cuantificar tomando en consideración un porcentaje del volumen de negocio total de la organización). Lo que hemos pretendido es presentar un avance de lo que el nuevo marco jurídico nos presenta y cuyo objetivo, lo adelantábamos al principio del presente artículo, no es otro que fortalecer los derechos de los interesados y adaptar la legislación comunitaria a los retos que plantean la globalización y las nuevas tecnologías en relación al tratamiento de datos.

Para terminar, avanzamos que en futuros artículos iremos ampliando o matizando esta información, conforme la propuesta del Reglamento siga su trámite legislativo, que sin duda, traerá modificaciones y alguna novedad al texto analizado.