EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS: DEL SIMPLE CUMPLIMIENTO A LA GESTIÓN DEL RIESGO

La **LOPD**, tal y como la conocemos hoy en día, tiene finalmente una fecha de caducidad. En base al último texto consolidado de diciembre de 2015, revisado y votado en Estrasburgo por la Comisión, el Consejo y el Parlamento, se tenía previsto que esta próxima primavera entrara en el Parlamento Europeo, donde se debatiría y se presentarían las últimas enmiendas. A finales de mayo salió a la luz el Nuevo Reglamento Europeo.

El largo camino se inició en 2010, hace ya unos 6 años, y el tiempo transcurrido muestra las múltiples dificultades y presiones que han existido, tanto desde dentro como desde fuera de Europa.

Actualmente, estamos funcionando con una Directiva Europea de 1995, que cada país ha traspuesto a nivel estatal, y que ha implicado grandes divergencias de aplicación entre los diferentes países. Ahora, el nuevo reglamento de protección de datos, será un texto único y de directa aplicación en todos los estados. A nivel español, y aun teniendo una de las regulaciones más avanzadas en este ámbito, los cambios que deberemos afrontar son importantes.

El punto clave del **nuevo reglamento de protección de datos** es una clara orientación a superar el modelo actual, modelo excesivamente formal. Dicho modelo se ha mostrado poco eficaz y eficiente, y en ciertos casos no ha conseguido dar respuesta a situaciones o nuevos retos asociados a las nuevas tecnologías. El modelo actual de cumplimiento se verá sustituido por un modelo de gestión. Se trata de gestionar. Primero gestionar para posteriormente cumplir.
A partir de la aprobación del nuevo reglamento se abrirá un periodo de transición hacía “El nuevo modelo de gobierno de protección de datos en Europa”. Dicho modelo se sustentará en dos pilares:

- El primero de ellos son las nuevas Autoridades de Supervisión de cada país, con más capacidades y más recursos, con un papel activo para que se cumpla la normativa dentro y fuera de Europa (recordar que también aplicará a las empresas no establecidas en territorio europeo pero que ofrezcan servicios dentro de la Unión). Se potenciará la coordinación de las diferentes autoridades para el tratamiento unificado de aspectos “supra” estatales.
- Creación del Consejo Europeo de **Protección de Datos**, por encima de las diferentes Autoridades de Supervisión, el cual, entre otras de sus funciones, partiendo del nuevo texto único, velará para la coherente aplicación en todos los estados.

Todo apunta a una forma muy diferente de afrontar los aspectos de protección de datos de carácter personal. Actualmente, y antes ya de la publicación del nuevo reglamento, se han empezado a anticipar acciones previstas para el presente ejercicio 2016: elaboración de directrices, guías más concretas y explicación de nuevos conceptos: derecho a la portabilidad, tratamiento del riesgo, esquemas de certificación y figura del responsable de

protección de datos. Y es que el nuevo reglamento trae consigo muchas novedades: derecho al olvido, derecho a la portabilidad, “Data Protection by design” y “Data Protection by default” o la nueva figura del DPO (Data Protection Officer), por citar algunos de ellos.

No es objetivo del presente artículo hacer una enumeración y repaso de todos ellos, sino apuntar las novedades más relevantes en materia de **seguridad de los datos**, y que nos puede aportar ideas sobre la magnitud del cambio que estamos a punto de afrontar:

- La definición de las medidas de seguridad a cumplir, irá en función de una evaluación de riesgos que las diferentes entidades deberán hacer. La nueva normativa se limita a enunciar que el Responsable del Tratamiento deberá aplicar aquellas medidas necesarias para garantizar el nivel de seguridad que requieran los datos. Para la aplicación de las medidas de seguridad, entraran en juego muchos conceptos como la finalidad y el alcance del tratamiento, la tipología y el volumen de datos personales, el propio coste de las medidas de seguridad, su proporcionalidad,…etc.

- Ampliación del perímetro de la seguridad de los datos. Hablamos de los propios datos pero ahora también de los diferentes elementos alrededor de éstos. Estamos hablando de conceptos como la residencia, que nos lleva a tratar aspectos como los planes de continuidad del negocio para poder dar respuesta y recuperarnos de los incidentes de seguridad.
- Revisión periódica de funcionamiento de las medidas de seguridad implantadas, y capacidad de justificar ante terceros que la entidad está tratando los datos con la seguridad que éstos requieren.
- Implantación y promoción de códigos de conducta y esquemas de certificación.
- Notificación de incidentes de **seguridad con datos personales** implicados. Notificaciones a realizar en dos direcciones:
    - Notificación a las **Autoridades de Supervisión**: En un periodo relativamente corto (72 horas) se debe dar, y por tanto estar preparado para obtener la información, importantes detalles de la incidencia: descripción del incidente, datos implicados, personas afectadas, impacto, medidas aplicadas (nuevas o previamente ya planificadas),…
    - Notificación a las personas implicadas: Siempre, previa notificación anterior, y de acuerdo a las instrucciones de la Autoridad, y a no ser que se exima de dicha obligación, comunicación del incidente a todas las personas implicadas.
- Finalmente, a nivel de sanciones, estamos hablando de unas importantes sanciones que realmente son muy elevadas. Éste ha sido uno de los principales aspectos que ha retrasado más la salida de la nueva normativa de protección de datos debido a las múltiples presiones recibidas por parte de las grandes multinacionales. Se prevén básicamente dos niveles de sanción:
    - Primer nivel: Hasta 10 millones de euros o 2 por ciento de la facturación a nivel mundial (por ejemplo por la no implantación de medidas de seguridad).
    - Segundo nivel: Hasta 20 millones de euros o 4 por ciento de la facturación a nivel mundial (afectación directa a principios y derechos de las personas).

- Adicionalmente, las Autoridades de Control, en caso de sanción, llevaran a cabo una supervisión de la aplicación de las medidas que se hayan estimado necesarias, y su no implantación, implicará nuevas sanciones.

Responsabilidad en la elección de colaboradores encargados de tratamiento

- Se ha escrito mucho sobre la responsabilidad en la elección de nuestros colaboradores y en la necesidad de colaborar sin riesgos.
- Para garantizar el cumplimiento de las disposiciones en el nuevo reglamento de protección de datos respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este **debe recurrir únicamente a encargados que ofrezcan suficientes garantías.**
- Por tanto, en el nuevo reglamento de Protección de Datos se exige **máxima diligencia en la elección de colaboradores con acceso a datos.**
- Deberás contratar solo aquellos que puedan acreditar conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento.
- La valoración y acreditación de estos colaboradores debe incluirse en el informe de impacto y el desarrollo del programa de privacidad por diseño.

Posibilidad de exigir indemnizaciones

- El nuevo reglamento de protección de datos contempla que el responsable o el encargado del tratamiento, **deba indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del Reglamento**.
- Veremos cómo repercute esta nueva posibilidad en el incremento de las denuncias que en la LOPD, **no preveían indemnización para los damnificados**, solo sanción para los responsables.
- Pero también señala que el responsable o el encargado deben quedar exentos de responsabilidad si se demuestra que en modo alguno **son responsables de los daños y perjuicios.**

Como vemos, el cambio de filosofía es muy importante, y debemos prepararnos para este nuevo escenario. Debemos estar en disposición de dar respuesta a las nuevas obligaciones, obligaciones nuevas en muchos aspectos, y con un rol de las nuevas **Autoridades de Supervisión** mucho más activo que el que estamos acostumbrados actualmente. Un nuevo escenario orientado a la gestión del riesgo aparece. Debemos

cambiar la actual forma de pensar para afrontar con éxito los nuevos **retos en protección de datos** de carácter personal, que por cierto, tenemos ya en la esquina.