

GDPR: ¿Una norma *totalmente disruptiva*?

El Reglamento General de Protección de Datos (RGPD o GDPR), sin duda ha revolucionado nuestro pequeño mundo. El alto importe de las sanciones, la inseguridad jurídica que plantea para las empresas y el conflicto que supone algunas de sus novedades con respecto a algunos modelos de negocio está generando mucha preocupación.

¿Pero realmente es un cambio tan relevante?

Hace unos días debatía con una clienta sobre este asunto. Ella afirmaba que le parece una norma que rompe drásticamente con todo lo anterior por sus novedades. Por mi parte, yo le decía que es indudable que supone un cambio y nos exige mucho más trabajo que antes, pero que, en el fondo, no es más que un maquillaje de lo anterior.

Ambos coincidimos en que los principios generales de la normativa, en esencia, siguen siendo los mismos. Pero para ella, las demás obligaciones que ha acuñado hacen que sea una norma totalmente novedosa.

Aprovecharé esta ocasión para profundizar en mi opinión al respecto analizando algunas de las principales novedades del Reglamento.

1.- Medidas de seguridad

Pasamos de un catálogo concreto de medidas de seguridad estructuradas por niveles a la necesidad de hacer un análisis de riesgos e implantar medidas adecuadas en función de estos riesgos.

Parece indiscutible que el cambio en este punto es radical. ¿Seguro?

Desde la óptica española, en parte sí. Pero comparemos el literal del RGPD con el de la Directiva 95/46, que fue derogada en 2016 por el propio RGPD.

Art. 17 Directiva 95/46	Art. 32 RGPD
Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse	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, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo [...]

En España (entiendo que por una cuestión de seguridad jurídica), se consideró necesario desarrollar este apartado con medidas concretas, aunque éstas siempre tuvieron la consideración de “mínimos exigibles”. Sin embargo, en otros países de la UE no se desarrolló.

En resumen, la diferencia es que ahora nos tenemos que tragar una inseguridad jurídica que hace un par de décadas se consideró inaceptable.

2.- Evaluaciones de impacto para la privacidad y consulta previa a la APD

Esta sí que es una auténtica novedad que no tenía nada parecido en la antigua normativa... o quizá sí.

Revisemos de nuevo el literal de las normas europeas.

Art. 20.1 Directiva 95/46	Art. 35 RGPD
Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán por que sean examinados antes del comienzo del tratamiento.	Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas , el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.
Art. 20.2 Directiva 95/46	Art. 36 RGPD
Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá consultar a la autoridad de control.	El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo

El asunto es que, al menos en España, no se traspuso de forma material el Artículo 20 de la Directiva 95/46.

Pero como puede verse, esta novedad tan novedosa no lo es tanto en el marco de la UE.

3.- Delegado de Protección de Datos

Todo el mundo sabe que esta figura no estaba prevista en la normativa anterior... y reconozco que este punto lo cogeré con alfileres, pero retrocedamos otra vez al 20.2 de la Directiva 95/46.

“Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento **o por el encargado de la protección de datos** quien, en caso de duda, deberá consultar a la autoridad de control.”

A primera vista, uno pensaría que este artículo se refiere al Encargado del Tratamiento y no al Delegado de Protección de Datos.

Sin embargo, si volvemos al literal de la Directiva 95/46, en concreto, a su artículo 18.2, se confirma que se refiere a un “proto-DPO”, al afirmar que los Estados miembros podrán simplificar u omitir la obligación de inscribir los ficheros en la autoridad de control:

“[...] cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, **un encargado de protección de los datos personales** que tenga por cometido [...]”

De hecho, sabemos que hay países como Alemania, cuya normativa ya exigía esta figura.

Y, dicho sea de paso, este mismo artículo ya deja claro que el registro interno de actividades de tratamiento, sin necesidad de inscripción pública, tampoco es una novedad del RGPD.

El Grupo de Trabajo del Artículo 29, también confirma la pre-existencia de la figura del DPO en sus Directrices sobre Evaluaciones de Impacto ([WP248 rev.1](#)), donde afirma lo siguiente:

“No será necesaria una EIPD para operaciones de tratamiento que hayan sido comprobadas por una autoridad de control o **el delegado de protección de datos, de conformidad con el artículo 20 de la Directiva 95/46/CE.**”

En conclusión, aunque desde España nos parezca un cambio sustancial, la norma marco europea ya consideraba esta figura en el año 95.

4.- El Interés Legítimo

Creo que este es el caso menos revelador, al menos dentro de los profesionales que nos dedicamos a la protección de datos.

La legitimidad del tratamiento por medio del denominado Interés Legítimo, estuvo siempre “de tapadillo” dentro de la legislación española. Más que “de tapadillo”, digamos que, en esta ocasión, nuestros legisladores nacionales pecaron por exceso y vincularon este interés legítimo con que los datos proviniesen de fuentes accesibles al público. Esto no se exigía en la normativa europea y tuvo que ser el Tribunal Supremo, previa consulta al TJUE, quien lo corrigiera (13 años después).

Quiero imaginar que el legislador español se excedió por un buen motivo, como era dotar de seguridad jurídica al uso de datos bajo un concepto jurídicamente indeterminado. Restringiendo dicho concepto a unos orígenes tasados de la información, se garantizaba la necesaria claridad de la norma. Pero fue en vano.

En todo caso, como hemos visto, no se trata de una novedad del RGPD.

5.- Responsabilidad Proactiva

Quizá podríamos buscar unos cuantos ejemplos más, pero hemos decidido cerrar este análisis con el denominado Principio de Responsabilidad Proactiva o Accountability.

Después de todo lo visto, no resulta sorprendente encontrarse con que esta inversión de la carga de la prueba tampoco es tan novedosa. Comparemos de nuevo el literal de la norma antigua con el de la nueva:

Art. 23.2 Directiva 95/46	Art. 5.2 RGPD
El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño	El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo.

Evidentemente, esto pisotea nuestro principio Constitucional a la Presunción de Inocencia, cuya aplicación es reconocida legal, doctrinal y jurisprudencialmente dentro del Derecho Administrativo Sancionador, y quizá por eso lo vemos como una **“novedad” tan preocupante.**

Sinceramente, espero que en este conflicto acaben triunfando las fuerzas del Bien.

Conclusión

Visto lo visto, digamos que si los autores de la Directiva 95/46 interpusiesen una reclamación por plagio de propiedad intelectual a los autores del RGPD, tendrían todas las de ganar (si estos derechos fueran de aplicación a este supuesto, claro).

Es cierto que en España algunos puntos nos afectan más, pero eso no es una cualidad del RGPD, sino, en todo caso, un defecto de nuestros legisladores nacionales.

Bendito defecto.

[José Carlos Moratilla](#)
[Departamento Legal](#)
[Área Seguridad de la Información](#)