IVAP
HERRI ARDURALARITZAREN
EUSKAL ERAKUNDEA

Erakunde autonomiaduna
Organismo Autónomo del
EUSKO JAURLARITZA
GOBIERNO VASCO

Rafael Jiménez Asensio

La aplicación del Reglamento (UE) de Protección de Datos en la Administración Pública: especial referencia a los entes locales

Rafael Jiménez Asensio
(Con la colaboración de Irati Labaka Garmendia)

IVAP
HERRI ARDURALARITZAREN EUSKAL ERAKUNDEA

Erakunde autonomiaduna
Organismo Autónomo del
EUSKO JAURLARITZA
GOBIERNO VASCO

La aplicación del Reglamento (UE) de Protección de Datos en la Administración Pública: especial referencia a los entes locales

Oñati, 2018

Edita: Instituto Vasco de Administración Pública
Herri-Arduralaritzaren Euskal Erakundea

ISBN: 978-84-7777-543-3

Fotocomposición e impresión: Grafo, S.A., Avda. Cervantes, 51-edificio 21 - 48970
Basauri (Bizkaia)

El presente documento, como se expone en el texto, tiene su origen en un trabajo que inicialmente fue difundido electrónicamente de forma conjunta por la *Federació de Municipis de Catalunya* y la *Associació Catalana de Municipis*, que llevaba por título *Manual-Guia sobre Impactes del RGPD en els ens locals*. Sin embargo, la actual versión cambia de forma sustantiva la orientación del texto (pues va dirigido a todas las Administraciones Públicas, aunque con especial referencia a los entes locales), modifica profundamente la primera parte, amplía y adapta bastantes contenidos de las partes segunda y tercera, así como incorpora un Epílogo («El futuro de la protección de datos en un entorno de revolución tecnológica»). Agradezco a Marta Iglesias, Responsable de Estudios y Publicaciones, la receptividad mostrada para publicar este texto por el Instituto Vasco de Administración Pública, que deberá ser adaptado una vez se apruebe de forma definitiva la nueva Ley Orgánica de Protección de Datos, hoy en día en tramitación en las Cortes Generales. También debo agradecer a Begoña Alberdi y Pili Arzuaga la buena gestión en el proceso de composición de este trabajo.

Índice

ISBN: 978-84-7777-543-3

Presentación

La finalidad del presente trabajo es ofrecer a los operadores de las Administraciones Públicas (y especialmente a los que trabajen en el mundo local), tanto políticos como empleados públicos, un documento en el que se sintetizan cuáles son las novedades más importantes del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (en lo sucesivo RGPD: https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80807)

El enfoque de este breve texto es predominantemente explicativo y no solo descriptivo. Se pretende que el lector comprenda el alcance de este nuevo marco regulador aprobado en su día por la Unión Europea y, asimismo, pueda identificar cuáles serán sus efectos aplicativos sobre las Administraciones Públicas a partir del 25 de mayo de 2018.

El análisis de esta cuestión se lleva a cabo mediante un estudio sistemático del RGPD donde se intercalan algunos documentos de interés (preferentemente de las autoridades de control o del Grupo de Trabajo del Artículo 29), así como se exponen algunas Ideas-fuerza y otras Recomendaciones u opiniones, que con el tiempo habrá de contrastarse su viabilidad o aplicabilidad. Tal como se verá, el modelo de protección de datos que pergeña el RGPD es lo suficientemente nuevo como para exigir un necesario período de transición para aquilatar sus contenidos y sus posibles interpretaciones.

ISBN: 978-84-7777-543-3

Por tanto, antes de precisar su contenido conviene adelantar lo que este documento no es. No es, en primer lugar, un texto para especialistas o personas que trabajan en el ámbito de la protección de datos, aunque algunas de las cuestiones que en este documento se tratan puedan asimismo interesarles o servirles, en su caso, de orientación o información adicional. Tampoco es, en segundo lugar, una Guía meramente aplicativa. En verdad, en estos últimos meses, auspiciados por las autoridades de control o por asociaciones de municipios (FEMP, FMC, AMC, etc.), están apareciendo diferentes Guías o documentos que cumplen esa finalidad orientativa. Recientemente, por ejemplo, ha sido publicado por la AEPD un documento titulado *Protección de Datos y Administración Local*, así como un buen número de Guías sobre contenidos específicos relativos al RGPD. Lo mismo están haciendo la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos, aunque en muchos casos son las tres Agencias las que conjuntamente comparten la elaboración de tales documentos. Una mera visita a sus páginas Web así lo confirman. En este texto se incluirán documentos o guías de las tres autoridades de control, aunque la AEPD ha sido hasta ahora la más activa en producción de tales textos. Y se reproducirán algunos de sus contenidos, esquemas o propuestas. Tales documentos o guías, así como las diferentes directrices elaboradas por el Grupo del Artículo 29 (y que se pueden consultar en la página Web de la AVPD: http://www.avpd.euskadi.eus/informacion/reglamento-general-de-proteccion-de-datos/s04-5273/es/) son, como se verá, de notable utilidad. En efecto, algunas recomendaciones o propuestas de estas autoridades de control se refieren a la implantación de aspectos relevantes del nuevo marco normativo, tales como el Registro de las Actividades de Tratamiento, la Seguridad en los tratamientos, el Análisis de Riesgos, la Evaluación de Impacto o el proceso de designación de la figura del Delegado de Protección de Datos, por traer a colación cinco ejemplos de indudable trascendencia para el funcionamiento del nuevo modelo de gestión de datos personales en las Administraciones Públicas.

Este documento pretende, por consiguiente, ser una herramienta básicamente pedagógica que facilite la introducción a ese nuevo modelo institucional y de gestión de datos personales y, asimismo, ayude principalmente a su cabal comprensión, pues no cabe duda alguna que el RGPD representa un notable **cambio de paradigma** en el modo y manera de comprender y aplicar esa cuestión en las Administraciones autonómicas, forales y en el nivel local de gobierno, así como en cualquier entidad perteneciente a su sector público institucional.

En todo caso, **aunque el presente trabajo solo se ocupa del RGPD, se recogerán también de forma adicional y con fines meramente informativos** (y un carácter obviamente provisional) **algunas referencias puntuales al texto del Proyecto de Ley Orgánica de Protección de Datos de carácter personal (PLOPD: https://bit.ly/2wC4Ay3)** actualmente en tramitación en las Cortes Generales, mediante el cual se complementa y adapta la normativa interna a las previsiones del RGPD. Cuando este texto se apruebe definitivamente y sea publicado como Ley Orgánica en el «BOE» habrá, sin duda, que volver a redefinir algunos aspectos puntuales de este documento. En el momento que se cierra este trabajo para su composición, el PLOPD se encuentra en fase de enmiendas en la Comisión correspondiente del Congreso de los Diputados. A tal efecto, se han presentado una amplia batería de enmiendas, por lo que los contenidos del proyecto que aquí se reflejan pueden sufrir algunas variaciones puntuales en el texto que definitivamente aprueben las Cortes Generales en los próximos meses (al parecer en el mes de julio próximo). Ver las enmiendas en Boletín Oficial de las Cortes Generales, Congreso Diputados, Serie A, núm. 13-2, de 18 de abril de 2018: https://bit.ly/2IhqFTV. Pero no cabe llamarse a engaño. Dada la naturaleza del instrumento normativo elegido (Reglamento de la Unión Europea), la posición esta vez de la LOPD será, a diferencia de la anterior, mucho más vicarial o complementaria. Ciertamente, tal como se dirá, a pesar de regularse esta materia en un Reglamento de la Unión Europea, el RGPD llama en más de cincuenta supuestos a que «sus normas sean especificadas o restringidas por el Derecho de los Estados miembros». En cualquier caso, como es sabido, el RGPD con carácter general tiene primacía aplicativa y entra, asimismo, en una serie de detalles en la regulación sustantiva tanto de principios, derechos como instrumentos o instituciones que la propia LOPD solo podrá reenviar a lo establecido en aquél.

Por consiguiente, frente a la situación anterior, **el operador** político, directivo o técnico **deberá actuar a partir de este nuevo marco con un binomio normativo que habrá de consultar en paralelo: RGPD y LOPD** (así como la Ley vasca que adapte, en su caso, la Ley 2/2004, de Ficheros de Datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, y de aquellas manifestaciones de la potestad reglamentaria desarrollen la LOPD).

Así, no cabe extrañarse de que este último texto (el actual PLOPD) lleve a cabo remisiones constantes a artículos del propio RGPD. El ré-

ISBN: 978-84-7777-543-3

gimen jurídico de protección de datos personales descansará, así, sobre dos «pantallas normativas» que se deben visualizar conjuntamente: RGPD y LOPD, sin perjuicio de tener también siempre presente lo que establezca, en su caso, la normativa autonómica. En todo caso, no habrá, ni se la espera, norma que sintetice esa regulación contenida en el binomio RGPD-LOPD, pues la posición de ambas fuentes del Derecho se asienta en dos subsistemas normativos y en el principio de primacía de la primera y, por tanto, de complemento de la segunda.

El contenido de la presente documento es muy sencillo de explicar.

El texto, según se afirmaba anteriormente, pretende ser un documento explicativo de lo que son los rasgos principales de la nueva normativa y de sus hipotéticos impactos sobre los gobiernos locales. Así, se estructura en tres grandes ejes:

- El primero analiza la transformación radical que se ha producido en el modelo de protección de datos de carácter personal.
- El segundo se ocupa de las cuestiones generales que trata el Reglamento: especialmente, principios y derechos. Los principios deben ser tenidos siempre en cuenta cuando se tratan datos por la Administración, los derechos son de las personas físicas, pero asimismo marcan territorio y establecen obligaciones a los poderes públicos.
- Y el tercero pone el foco de atención en los elementos centrales del nuevo modelo institucional y de gestión de protección de datos personales y su aplicación sobre la Administración Pública y, en concreto, sobre los gobiernos locales. Es en este último punto donde las novedades han sido más relevantes, pues el enfoque de riesgos por el que opta el RGPD requiere un arsenal de instrumentos para poderse hacer efectivo.

No se tratarán en este documento, al menos directamente, aquellos aspectos que, en principio, inciden menos directamente sobre la actuación de las Administraciones Públicas y, en concreto, sobre los gobiernos locales. Por ejemplo, no se aborda un tratamiento específico del Capitulo V (transferencias de datos personales a terceros países u organizaciones internacionales) o del Capítulo VII (Cooperación y coherencia), entre otros temas, sin perjuicio de que todas esas previsiones normativas se deben tener completamente en cuenta en el tratamiento de datos personales por el sector público, más aún en un entorno de globalización de los datos y de cruce permanente de información.

Quiero agradecer aquí las aportaciones o sugerencias que al contenido inicial de este trabajo llevó a cabo mi buen amigo Iñaki Vicuña, Director del CENDOJ (Consejo General del Poder Judicial) y, en su día, también Director de la Agencia Vasca de Protección de Datos, así como las aportaciones que también hizo a un primer borrador Ascen Moro del Ayuntamiento de Sant Feliu de Llobregat. También cabe resaltar la ayuda prestada por Irati Labaka Garmendia en la parte documental y en la revisión del documento. En todo caso, los errores u omisiones solo se pueden imputar a quien ha estado encargado de redactar el presente texto.

Solo quisiera añadir, finalmente, que una primera versión de este texto, fue editada inicialmente en catalán y después también en castellano por la FMC-AMC con el título *Manual-Guía sobre impactos del RGPD en los entes locales*. Pueden consultarse estos documentos en los siguientes enlaces: https://www.fmc.cat/novetats-ficha.asp?id=25009&id2=1 / https://www.aoc.cat/2018/04/23/fmc-i-acm-presenten-una-guia-sobre-els-impactes-del-reglament-europeu-de-proteccio-de-dades/

En cualquier caso, el presente documento cambia la orientación del texto inicial (pues va dirigido a cualquier Administración Pública, sea autonómica, foral o local, aunque con más referencias puntuales a esta última), amplía notablemente tanto la parte primera del texto como el epílogo del mismo, que es completamente nuevo, así como adapta y desarrolla algunos de los contenidos de la parte central del trabajo. Especialmente, este documento tiene en cuenta la realidad político-institucional vasca, su marco normativo y la actuación de la Agencia Vasca de Protección de Datos en el impulso y desarrollo de la aplicación del RGPD, que a todas luces tendrá un protagonismo estelar en ese proceso. Por tanto, con las advertencias realizadas, se trata de un texto nuevo que, no obstante, bebe parcialmente de la fuente antes citada.

Donostia-San Sebastián, mayo 2018
estudiosectorpublico@gmail.com
www.estudiosectorpublico.com

I.

Líneas-fuerza del nuevo marco normativo de la UE en materia de protección de datos de carácter personal

1. ¿POR QUÉ UNA NUEVA REGULACIÓN EUROPEA?

> *«Hay una cosa cierta al menos y es que también en este caso lo que se impone es la palabra* ***regulación*** *frente a una mercantilización y una desregulación del mundo sin equivalente alguno en la historia de la humanidad»*
>
> (Luc Ferry, *La revolución transhumanista. Cómo la tecnología y la uberización del mundo van a transformar nuestras vidas*, Alianza Editorial, 2017, p. 154)

La necesidad objetiva de la nueva regulación europea en materia de protección de datos de carácter personal surge del propio contexto tecnológico y de su evolución en las dos últimas décadas. En efecto, en los

ISBN: 978-84-7777-543-3

más de veinte años transcurridos desde 1995 (fecha de aprobación de la Directiva 95/46/CE) hasta 2016 (fecha de entrada en vigor del Reglamento 2016/679, del Parlamento Europeo y del Consejo) la digitalización y la revolución tecnológica, así como la globalización y transferencia internacional de los propios datos, ha generando nuevos e importantes retos para la protección de los datos personales y, en particular, para los derechos y libertades de los ciudadanos. Y nada sabemos con certeza, aunque lo intuyamos, sobre qué pasará en un futuro mediato. Innumerables incógnitas, incertidumbres y no menos perplejidades rodean el desarrollo o profundización de la automatización, de la inteligencia artificial y del Big Data, por no hablar de los ordenadores computacionales, que anuncian el fin de la privacidad. Las consecuencias de todos esos procesos se mueven aún en una escala desconocida.

En efecto, la aceleración de los procesos tecnológicos y su impacto sobre los datos personales es, hoy en día, una realidad incontestable, que irá creciendo o desarrollándose cada vez más y a ritmos más intensos, por lo que esta nueva regulación no solo se dicta para afrontar los retos del presente, sino en especial también para hacer frente a los grandes desafíos del futuro en materia de protección de datos y de garantía de los derechos y libertades de los ciudadanos, ámbitos que en estos momentos están comenzando a ser objeto de una erosión nunca conocida hasta la fecha. El riesgo que se corre es que tal regulación llegue tarde o que pronto se quede corta, sobre todo por las dificultades de adaptación que el marco regulador europeo presenta.

Sin embargo, la orientación —como inmediatamente se dirá— preferentemente *preventiva* o situada en un *enfoque de riesgos* precisamente tiende a evitar que los responsables y encargados de los diferentes tratamientos se encuentren ante situaciones nuevas que no puedan hacer frente y que, por consiguiente, esos nuevos e inciertos contextos que se produzcan en el ámbito tecnológico puedan erosionar los derechos de las personas físicas a través de la manipulación o uso torticero de los datos personales. Ante la evidente situación de incertidumbre que se atisba frente al desarrollo efectivo, las secuelas o efectos de la revolución tecnológica, ese enfoque anticipatorio o preventivo era la solución más idónea por parte del poder normativo europeo. Y este fenómeno de revolución acelerada, cuyas consecuencias mediatas e inmediatas están aún por descubrir, no podía ser afrontado de otro modo. El viejo modelo de control quedaba total-

mente desfasado y había que prepararse para un largo e inevitable escenario de incertidumbre.

Tampoco conviene olvidar que cuando se aprobó la Directiva 95/46/CE el desarrollo de Internet era mucho menor. Las redes sociales y buena parte de las compañías tecnológicas no habían nacido o se encontraban en un estadio de desarrollo mucho menor. En pocos años, **tras superarse el umbral del siglo** xx **y dar sus primeros pasos el siglo** xxi**, el escenario de protección de datos comenzó a cambiar de forma radical y a unas velocidades de vértigo**. Los datos personales, muchas veces con plena anuencia y más bien con fuerte desconocimiento de sus consecuencias por parte de las personas físicas, fueron «entregados» por la ciudadanía a esas grandes compañías tecnológicas o redes sociales que ofrecían servicios de búsqueda o intermediación aparentemente gratuitos. Tal como acertadamente reconoció Luc Ferry, «si es gratuito es porque tú eres el producto; si no pagamos nada, la mercancía somos nosotros». Más claro no se puede decir.

Uno de los documentos más importantes que dio inicio al cambio normativo en materia de protección de datos en la Unión Europea fue la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, titulada ***Un enfoque global de la protección de los datos personales en la Unión Europea***, **COM/2010/0609 final**. Allí ya se ponía el foco en los trascendentales cambios que se habían producido en materia de protección de datos, y a los que obviamente había que hacer frente desde las instituciones europeas.

> *COMUNICACIÓN (2010/0609) «Un enfoque global de la protección de los datos personales en la Unión Europea»*
>
> *En la actualidad,* ***la tecnología permite a los ciudadanos intercambiar fácilmente información con respecto a sus comportamientos y sus preferencias,*** *y hacerla pública a nivel mundial a una escala sin precedentes.* ***Las redes sociales****, con centenares de millones de miembros en todo el mundo,* ***constituyen seguramente el ejemplo más evidente de este fenómeno, sin ser el único.*** *La computación en nube, esto es, informática basada en Internet en la que los programas, los*

ISBN: 978-84-7777-543-3

recursos compartidos y la información se encuentran en servidores remotos, también podría plantear retos para la protección de datos, dado que puede implicar la pérdida del control por parte de los individuos de su información potencialmente sensible cuando almacenan sus datos utilizando programas alojados en servidores ajenos. **Un reciente estudio ha confirmado que** *las autoridades responsables de la protección de datos, las organizaciones profesionales y las asociaciones de consumidores coinciden en que* **los riesgos para la protección de la intimidad y los datos personales están aumentando con las actividades en línea.**

Paralelamente, **los métodos de recogida de los datos personales son cada vez más complicados y se detectan con más dificultad**. *Por ejemplo, la utilización de herramientas sofisticadas permite a los agentes económicos localizar mejor a las personas, mediante el registro de su comportamiento. El mayor recurso a procedimientos que permiten la recogida automática de datos, como el pago electrónico de billetes, el cobro de peajes en carreteras, o instrumentos de geolocalización facilitan la determinación de la ubicación de un individuo por el mero uso por su parte de un dispositivo móvil.* **Las autoridades públicas también utilizan cada vez más datos personales con distintos fines***: para buscar personas cuando se declara una enfermedad transmisible, para prevenir y luchar más eficazmente contra el terrorismo y la delincuencia, para gestionar su régimen de seguridad social o a efectos fiscales, en el marco de sus aplicaciones de administración en línea, etc.*

Si esto era así en 2010 qué puede decirse en 2018 y qué podrá suceder en 2025 o 2030. Como también se dijo por un autor, «la fuente precisa del poder de Facebook son los algoritmos» (Franklin Foer, *Un mundo sin ideas*, Paidós, 2017). Larry Page lo expresó de forma mucho más cruda: «**El algoritmo es el rey, un soberano frío y sin pulso**». Y, en verdad, lo que todas estas compañías tecnológicas hacen es —como se dijo gráficamente— «torturar a los datos hasta que confiesen». Nada hay que sorprenderse, por tanto, en este nuevo contexto, donde además los escenarios de futuro, por mucha prospectiva que se haga, son impredecibles. Por tanto, **se hace necesario asimismo** un mejor co-

nocimiento **por parte de las personas físicas** de cuáles son los procedimientos de tratamiento de datos, así como especialmente **disponer de una mayor capacidad de (auto)control de la protección de datos personales**, algo que se debe transmitir por diferentes vías, pero que resulta un proceso de sensibilización en el que el sector público (por ejemplo, el ámbito educativo) tiene un rol sustancial.

Nadie puede evitar que, en determinadas circunstancias, se produzca una manipulación de datos personales con fines absolutamente espurios (recuérdese el reciente caso *Cambridge Analytica*), algo que afecta principalmente a las grandes compañías tecnológicas, pero que advierte claramente de una tendencia ya fuertemente arraigada de mal uso o uso para fines espurios de los datos personales por las grandes compañías tecnológicas (en régimen de cuasi monopolio global) y por las empresas de intermediación, cuando no también por parte de algunos Estados que están en la mente de cualquier persona mínimamente informada. **En este acelerado contexto, el papel del Sector Público y, particularmente, de la Administración Pública, adquiere un rol de gran importancia para preservar los derechos y libertades de la ciudadanía**. La protección de los datos personales que maneja cotidianamente cualquier nivel de gobierno se transforma en un reto de alto valor democrático.

La idea está perfectamente expresada en el ***Considerando 6 del RGPD:***

«La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales»

ISBN: 978-84-7777-543-3

2. ¿CUÁLES SON LOS MOTIVOS POR LOS QUE SE HA DEROGADO LA DIRECTIVA DE 95/46/CE Y SE HA APROBADO EL REGLAMENTO (UE) 2016/679?

> *«No es de extrañar que Alphabet (Google) ya no hurgue en nuestros correos electrónicos personales para mostrarnos anuncios personalizados: ya sabe todo de cada uno de nosotros y puede prescindir de más información (…) Es decir, en la medida en que el entorno normativo se vuelva más problemático y/o el mercado publicitario se desacelere (…) la compañía tendría un modelo de negocio muy robusto: vender "servicios inteligentes" (IA), tanto a ciudadanos como a gobiernos»*
>
> (Evgeny Morozov, *Capitalismo «Big Tech» ¿Welfare o neofeudalismo digital?* Enclave, 2018 pp. 23-24)

La derogación de la Directiva 96/45/CE y su sustitución por el RGPD no es una operación normativa menor. El cambio de instrumento regulador obedece, tal como se ha visto, a razones de contexto y a la necesidad objetiva de establecer un Reglamento (UE) que, como es sabido, es una disposición normativa europea que tiene un alcance general, es obligatoria en todos sus elementos y directamente aplicable.

No cabe duda que, frente al fenómeno descrito en el apartado anterior (el acelerado proceso de revolución tecnológica y de digitalización, así como sus enormes impactos sobre los datos personales), la única solución viable es la *regulación*. El proceso de mercantilización de los datos al cual contribuimos nosotros mismos «sin quererlo» revelando enormes cantidades de información, implica que, tal como se ha dicho, nuestras vidas se están *datificando.* Algunos ejemplos de ese singular proceso de «datificación» (o de entrega «libre» y «desinteresada» de datos personales) los ha recogido Colin Strong en un reciente libro (*Big Data a escala humana,* Melusina, 2018):

- *Datificación de los sentimientos/emociones*
- *Datificación de las interacciones/relaciones*
- *Datificación del habla*
- *Datificación de la actividad «offline»*
- *Datificación de la cultura*

Toda esa actividad intrusiva de los datos convenientemente «cocinados» puede, sin duda, afectar (y de hecho afecta, aunque con consecuencias aún imprevisibles) a los derechos fundamentales de las personas físicas y ya no solo a la intimidad o a la privacidad, sino a la inmensa mayoría de ellos. **Es bien cierto, no obstante, que la Administración Pública y las entidades de su sector público** no tienen ni de lejos el comportamiento mercantilista que puedan mostrar determinadas grandes empresas tecnológicas, pero también lo es que **pueden tratar (y de hecho tratan) gran cantidad de datos personales (un volumen considerable) que, en determinados contextos, pueden ser causa o provocar situaciones de riesgo evidente**.

Asimismo, es también obvio que **el sector público trata en no pocas ocasiones «categorías especiales de datos» (datos sensibles)**, por utilizar la terminología del Reglamento UE. **Todo ello requiere a los responsables y encargados del tratamiento en el sector público especial diligencia en tales procesos, pero en particular fomentar una cultura y actividad preventiva tanto en el diseño de los procesos de tratamiento como por defecto** (esto, es de manera permanente, analizando en cada caso y circunstancia la necesidad de tales tratamientos), aplicando todas las medidas técnicas y organizativas que estén a su alcance para salvaguardar los derechos fundamentales de las personas físicas (el objetivo central, no se olvide, del RGPD).

Por consiguiente, **la regulación que se ha llevado a cabo a través del Reglamento (UE) 2016/679 es particularmente importante por lo que afecta al sector público**. Pero de inmediato cabe afirmar que, sin perjuicio de que se aplique también al sector público (a lo que el Reglamento denomina «autoridades y organismos públicos»), no es menos cierto que **el foco central de preocupación de esa disposición normativa de la Unión Europea es el riesgo que para la protección de los derechos fundamentales y, en especial, la protección de datos de las personas físicas, se pueda producir como consecuencia del tratamiento masivo de datos, del cruce entre estos datos dirigido entre otras cosas a la elaboración de «perfiles» y de las observaciones masivas derivadas de los datos**. Y esto es algo que, también en principio, potencialmente lo están llevando a cabo las grandes empresas tecnológicas y todas aquellas empresas que de una u otra forma participan en esos procesos de recogida, tratamiento y comercialización futura de tales datos. El RGPD establece una redefinición de la noción de dato personal y una noción de tratamiento amplia y exhaustiva (artículo 4).

ISBN: 978-84-7777-543-3

La entrada en vigor del Reglamento UE 2016/679, como es sabido, se produjo a los veinte días de su publicación en el DOUE, pero su plena aplicabilidad es a partir del 25 de mayo de 2018 (artículo 99 RGPD).

En los **Considerandos 9 a 13 del RGPD se explicitan cuáles han sido los motivos que han justificado el cambio de instrumento normativo**. Entre los que caben citar los siguientes:

- —**La aplicación de la Directiva 1995 ha sido fragmentaria y desigual**, mientras que los riesgos para la protección de datos, tal como se ha visto, son cada vez mayores. Y lo serán conforme el tiempo avance.
- —**Se quiere garantizar un nivel uniforme y elevado de protección de datos personales, y que sea además equivalente en todos los Estados miembros**. La aplicación de las normas de protección de datos se pretende que sea coherente y homogénea. La Directiva 95/46/CE no garantizaba ese objetivo y esa fue una de las causas por las que se impulsó ese profundo cambio de instrumento normativo.
- —**La protección efectiva de los datos personales exige reforzar las obligaciones de quienes los tratan**, reconocer poderes equivalentes para supervisar y garantizar su cumplimiento, así como que las infracciones se castiguen con sanciones equivalentes. **El endurecimiento del régimen sancionador es uno de los presupuestos de apoyo de tal normativa**, aunque se modula en su aplicación a las «autoridades y organismos públicos» en función de lo que determine la legislación de cada Estado miembro.
- —**Hay base jurídica para esta regulación en el artículo 16. 2 del TFUE**. Aunque el derecho fundamental ya estaba recogido (luego trasladado al propio TFUE) en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.
- —Era, por tanto, necesario regular esta materia por un Reglamento que **proporcionará seguridad jurídica y transparencia**.

El Consejo de Estado, en su dictamen 757/2017, de 26 de octubre de 2017, sintetizó en una serie de ideas-fuerza el recurso al instrumento normativo del Reglamento, norma obligatoria en todos sus elementos y directamente aplicable en todos los Estados miembros (artículo 288 TFUE), como medio necesario para llevar a cabo esa reducción de las divergencias normativas que se habían producido con la aplicación de la Directiva 95/46/CE.

Por qué se ha elegido el instrumento del Reglamento UE frente a la Directiva para regular la protección de datos: ideas-fuerza del Dictamen 757/2017 del Consejo de Estado:

— *«Esa* **aplicabilidad directa de los Reglamentos exige su entrada en vigor y su aplicación sin necesidad de ninguna medida de incorporación al Derecho nacional***».*

— *«Los* **Estados miembros** *están obligados (…) a no obstaculizar el efecto directo propio de los Reglamentos, siendo el "***respeto escrupuloso** *de este deber" una* **condición indispensable "para la aplicación simultánea y uniforme" de las reglas contenidas en los Reglamentos** *de la Unión en el conjunto de esta.»*

— *«***El Reglamento 2016/679 pasa así a ser la norma principal para la regulación de datos en la Unión Europea***, directamente aplicable en todos los Estados miembros sin necesidad de normas internas de trasposición.»*

— *«De esta forma,* **un derecho fundamental protegido por el artículo 18.4 de la Constitución española va a ser directa y principalmente regulado en una norma europea***, con un papel únicamente de desarrollo o complemento de las normas nacionales.»*

— *«Ello implica también un traslado parcial del canon constitucional de protección del derecho fundamental que, en cuanto se refiere a actividades regidas por el Derecho de la Unión, deberá regirse por la Carta de Derechos Fundamentales de la Unión Europea y por la interpretación que realice el Tribunal de Justicia de la Unión.»*

— *«***La legislación nacional en materia de protección de datos, por tanto, debe necesariamente modificarse para adaptarla a este nuevo contexto normativo** *europeo antes de la entrada en vigor del Reglamento, que se producirá el 25 de mayo de 2018».*

ISBN: 978-84-7777-543-3

> — «**Esa adaptación implica**, *por motivos de seguridad jurídica,* **la necesaria derogación de las normas nacionales que sean incompatibles con el nuevo Reglamento (y) llevar a cabo una segunda tarea de depuración del ordenamiento nacional**, *del que deben igualmente eliminarse cuantas disposiciones hayan devenido redundantes como consecuencia del efecto directo de aquél, en la medida en que puedan poner en cuestión esa aplicación directa del Reglamento».*
> — *«En fin,* **la adaptación de la legislación nacional puede también exigir, en algunos casos puntuales, la adopción de nuevas disposiciones llamadas a completar o aclarar la regulación europea.** *La aplicabilidad directa del Reglamento no excluye, en efecto, esa labor puntual de complemento de la normativa de los Estados miembros».*
> — *«Así lo hace el Reglamento general de protección de datos. Pese a su intensa vocación armonizadora, el Reglamento contiene el menos 56 remisiones de diverso alcance al Derecho de los Estados miembros, permitiendo a estos adaptar la regulación europea, en distintos casos, al contexto nacional, o fijar exenciones, derogaciones o condiciones específicas para determinadas categorías de tratamiento de datos».*

Por consiguiente, **el operador jurídico** o técnico debe ser plenamente consciente de que, en este nuevo contexto normativo de protección de datos personales y a diferencia del marco normativo anterior (en el que la LOPD era la referencia determinante), **deberá trabajar con dos herramientas normativas «en paralelo»**: **una de carácter principal**, reforzada además por la primacía del Derecho de la Unión Europea frente al Derecho de los Estados miembros, **como es el Reglamento (UE) 2016/679, mientras que la otra será la futura LOPD** (actualmente en proceso de tramitación parlamentaria) **que se limitará a «completar o aclarar» la regulación europea**, así como a establecer determinadas excepciones solo cuando esté habilitada específicamente para ello por la normativa europea.

El resultado, como se dirá en su momento, es bien obvio: **el Reglamento (UE) 2016/679 se convierte en la norma de cabecera en**

materia de protección de datos y la (futura) LOPD será una disposición normativa, por mucho que se califique de «orgánica», de carácter complementario o de desarrollo. Es más, si la Ley Orgánica está llamada a desarrollar los derechos fundamentales y libertades públicas recogidos en la sección primera del capítulo segundo del título primero de la Constitución, en este caso el desarrollo de este derecho fundamental, con la base jurídica que le da el propio TFUE y la CDFUE, se llevará a cabo por el propio Reglamento UE y no por la LOPD, cuyo proyecto realiza un mero reenvío, al menos en lo que a las dimensiones del derecho a la protección de datos respecta, a los establecido en la disposición normativa europea.

Ello no implica que la actualmente vigente LOPD (Ley Orgánica 15/1999, de 30 de diciembre), así como su Reglamento de desarrollo (real Decreto 1720/2007, de 21 de diciembre), ya no sean normas vigentes, sino que una parte relevante de su contenido ha quedado afectado por la nueva regulación recogida en el RGPD y, por consiguiente, ya no resulta de aplicación, al tener primacía aplicativa la normativa recogida en el Reglamento (UE) 2016/679. Por ello urgía la aprobación de una nueva LOPD, aunque el legislador español ha estado poco atento a esa exigencia y el 25 de mayo de 2018 no tendrá adaptada la normativa interna a las previsiones del nuevo marco normativo europeo. Y por ello también es necesaria la adaptación del Reglamento que la desarrolla (Real Decreto 1720/2007), algo que cabe presumir tardará bastante más tiempo. Mientras tanto, para los operadores del sector público, responsables, funcionarios y resto de empleados públicos, se abre un escenario no exento de dificultades aplicativas en algunos casos, que habrá de sortearse como mejor se pueda. En todo caso, parece que en unos pocos meses estará aprobada la nueva LOPD, lo que al menos dotará de una mayor seguridad jurídica a determinadas actuaciones.

3. EL NUEVO MARCO NORMATIVO DEL RGPD COMO CAMBIO DE PARADIGMA

> *«Como los malos estudiantes, la mayoría de empresas españolas (y no digo nada de la Administración) no han hecho los deberes y ahora se acuerdan de Santa Bárbara, o de Santo Dato, cuando ya se escuchan los primeros truenos».*
>
> (Borja Adsuara Varela. *Protección de Datos: Quedan solo cuatro meses para ponerse al día*, Retina-El País, enero 2018)

ISBN: 978-84-7777-543-3

Este punto requiere un desarrollo algo más detenido. En efecto, la nota distintiva del actual marco normativo (RGPD-futura LOPD) frente al vigente hasta ahora (Directiva-LOPD) reside en transitar ***desde un modelo reactivo a un modelo proactivo o centrado en el «enfoque de riesgos».*** Ese cambio de «filosofía» de la nueva regulación europea está perfectamente descrito en los Considerandos del RGPD, así como se refleja tangencialmente en diferentes disposiciones normativas de ese Reglamento europeo.

Las razones de ese tránsito en la concepción del problema han sido expuestas anteriormente, pero todas ellas **tienen que ver con dos factores sustantivos**:

a) **La posición dominante de las grandes compañías tecnológicas que tienen una posición de cuasi monopolio en todo lo que afecta a los datos personales** con un volumen de información cada vez más abrumador, lo que puede tener serias consecuencias sobre los derechos de la persona y la propia subsistencia del Estado democrático tal como lo hemos concebido tradicionalmente;
b) **El acelerado e incierto desarrollo tecnológico que, basado en el dato personal y en los algoritmos, está inaugurando una nueva revolución tecnológica de resultados altamente inciertos**, un contexto que exige incidir especialmente en la prevención o en el denominado «enfoque de riesgos», algo que obligará a las Administraciones Públicas (en cuanto organizaciones que tratan gran cantidad de datos personales y algunas veces datos de carácter sensible) a establecer un registro de actividades de tratamiento, incrementar las medidas de seguridad dirigidas a proteger los derechos fundamentales de las personas que sean titulares de esos datos, así como a llevar a cabo una serie de análisis de riesgos y, en su caso, evaluaciones de impacto, aparte de dotarse de una arquitectura organizativa dirigida a cumplir esos fines establecidos por el Reglamento (funciones de los responsables y encargados del tratamiento; la figura del Delegado de Protección de Datos; el papel de las autoridades de control; etc.).

En cierta medida se puede afirmar que **se traslada a la protección de datos de carácter personal** (aunque con algunas limitaciones, según se verá) **el esquema propio de la *política de compliance*, en el que la dimensión preventiva o anticipadora es una de las claves de**

bóveda del modelo que se pretende construir. Ante la más que evidente incertidumbre que plantea el desarrollo tecnológico el consejo que cabe transmitir es estar siempre alerta, también en el ámbito de lo publico.

Y la inversión en esta dimensión preventiva es razonable y lógica, pues está estrechamente unida a ese escenario de incertidumbre sobre cuál pueda ser el desarrollo futuro de la tecnología y qué implicaciones podrá tener sobre los datos personales y el uso que finalmente se haga de ellos. En esa clave hay que entender todos aquellos elementos que van dirigidos a la protección de datos desde el diseño y por defecto, a evaluar los impactos de determinados tratamientos de datos personales o a llevar a cabo, en su caso, las consultas que se deben hacer a las autoridades de control. Y en la misma línea cabe incluir las obligaciones de notificar a las autoridades de control y a las personas físicas afectadas los problemas de seguridad como consecuencia de lo que se ha denominado como el *breach data* (las caídas del sistema, los ciberataques) o cualquier otra circunstancia que pueda poner en riesgo los datos personales que se estén tratando por la Administración Pública o por las entidades de su sector público.

Como se ha venido reconociendo, también por la AEPD (Informe sobre el proyecto de LOPD), en verdad con este nuevo marco normativo impulsado por el RGPD se ha producido un *auténtico cambio de paradigma* en el modo y manera de gestionar los datos personales con innegables consecuencias, no solo presentes sino sobre todo futuras. Se puede afirmar, sin riesgo a equivocarse que el RGPD es una disposición normativa que afronta una regulación con vistas a resolver problemas inmediatos, pero que se dota de los instrumentos necesarios para enfrentarse a los innumerables retos e incertidumbres que se abren en el futuro.

Pero el RGPD se enmarca en un contexto ineludible de economía digital, en la que el dato es el elemento sustantivo. Y no pretende, en ningún caso, obstaculizar ese desarrollo. A tal efecto, uno de los objetivos del RGPD es también establecer «las normas relativas a la libre circulación de datos personales». Por tanto, como también prevé el artículo 1.3 RGPD: «la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta a la protección de datos personales. Pero todo ello de acuerdo con lo determinado en el propio RGPD, que tiene como objeto último la protección de esos datos personales y de los derechos de los ciudadanos. En esa

ISBN: 978-84-7777-543-3

lógica hay que entender asimismo la amplia regulación normativa que prevé el RGPD en materia de transferencia de datos personales a otros países u organismos internacionales (Capítulo V).

Ambas ideas citadas tienen perfecto reflejo en los Considerandos 7 y 101 del RGPD. Veamos.

> Considerando 7:
>
> «Estos avances requieren un marco normativo más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económico y las autoridades públicas».

> Considerando 101:
>
> «Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacional. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal (…) En todo caso, las transferencias a terceros países y organismos internacionales solo puede llevarse a cabo de plena conformidad con el presente Reglamento».

La Unión Europea ha sido la primera instancia que se ha inclinado por una regulación «regional» de la protección de datos personales y por exigir a todas esas grandes empresas tecnológicas (así como al resto de sujetos obligados, entre ellos las Administraciones Públicas) el cumplimiento de una exigente normativa. Esa regulación normativa está obligando a esas empresas tecnológicas que actúan de forma globalizada a adaptar su funcionamiento al Reglamento de la Unión Europea, al menos en determinados espacios geo-

gráficos entre los que se encuentra, sin duda, el continente europeo. El paso adelante es significativo. Su ejemplo puede cundir y es necesario que así sea. Estados Unidos aún no lo ha hecho, sin perjuicio de que la reciente comparecencia en el Senado del creador de *Facebook,* Mark Zuckerberg, a cuenta del escándalo de *Cambridge Analytica* (y de «la fuga de datos» que implicó) haya planteado abiertamente esa necesidad, puesto que dejar en manos de la autorregulación un tema de tan alta sensibilidad para el vigor de los derechos fundamentales de las personas físicas en el Estado democrático es jugar sencillamente con fuego o arriesgarse a ver cómo se pueden remover los cimientos del Estado Constitucional.

El nuevo marco normativo se asienta sobre una serie de principios que todos los responsables y encargados del tratamiento deben respetar, algunos de ellos redefinidos, y asimismo con un nuevo catálogo ampliado de dimensiones de derechos específicos vinculados con la protección de datos personales, que deberán ser garantizados en su ejercicio por las Administraciones Públicas. También hay nuevas facetas de tales derechos (derecho a la limitación de los tratamientos, derechos a la portabilidad de datos o derecho al olvido) y redefinición de algunos otros de ellos. La Sentencia del TJUE de 2014 (Google contra España) tuvo en este punto importancia destacable, al menos para impulsar ese denominado «derecho al olvido», una redefinición del derecho a la cancelación de datos personales, ya existente.

En todo caso, la Administración Pública, a través de los responsables y encargados del tratamiento, debe cumplir fielmente los principios relativos al tratamiento, debiendo estos informar toda la actuación pública en cualquier tratamiento de datos personales (artículo 5 RGPD) y, especialmente, teniendo en cuenta la «base jurídica» o «licitud del tratamiento», sea esta el consentimiento del interesado o afectado (en los términos que se recogen en el citado RGPD), el cumplimiento de una obligación legal aplicable al responsable de tratamiento o, en su caso, el cumplimiento de una misión realizada en interés público o en el ejercicio de los poderes públicos conferidos al responsable de tratamiento (artículo 6 RGPD, letras a), c) y e). Aspectos estos últimos determinantes para que la Administración Pública pueda tratar legítimamente los datos personales.

Con ser importante esa cuestión, en el campo de la Administración Pública resulta trascendental la articulación a través del Reglamento (UE) 2016/679 de una serie de elementos perfectamente es-

ISBN: 978-84-7777-543-3

tructurados que tienden a salvaguardar la orientación principal de esa normativa: prevenir riesgos futuros en el tratamiento de datos personales. Gran parte de esa arquitectura de elementos instrumentales o de gestión se encuadran en esa *política de compliance* sobre la cual se inspira el modelo, pero otros disponen de autonomía propia, aunque encuentran su pleno sentido en ese enfoque de riesgos reiteradamente citado.

En verdad, el RGPD combina acertadamente instrumentos de gestión de protección de datos basados en ese enfoque de riesgos, con una redefinición del modelo institucional que fortalece el papel de las autoridades de control y articula un conjunto de medidas sancionadoras con fuerte componente de disuasión para evitar la erosión de los derechos fundamentales de la persona física a través del tratamiento de datos personales.

En efecto, en esta lógica se enmarcan diferentes instrumentos o instituciones que se articulan dentro de lo que se podría denominar como un nuevo modelo institucional y de gestión de las protección de datos en las organizaciones públicas, que descansa principalmente sobre una serie de ejes de la configuración del sistema de protección de datos a partir del Reglamento (UE) 2016/679.

Este nuevo modelo de gestión de protección de datos debe ser seguido fielmente por parte de las Administraciones Públicas y por las entidades de su sector público, puesto que en este caso todos y cada uno de esos elementos (con algunas singularidades tales como la necesidad de llevar a cabo evaluaciones de impacto, las excepciones en los supuestos del régimen se supervisión de códigos de conducta o las derivadas en materia de el régimen específico de sanciones que se pueda definir, entre otras) se aplican también a las organizaciones públicas

ELEMENTOS DEL NUEVO MODELO DE GESTIÓN DE DATOS PERSONALES EN LAS ADMINISTRACIONES PÚBLICAS

1. Nuevo rol o nuevo marco de responsabilidades del responsable y, particularmente, del encargado del tratamiento de datos. Particularmente todo lo relativo a la protección de datos desde el diseño y por defecto.

2. **Registro de las actividades de tratamiento**. Instrumento de obligada existencia, con unas excepciones muy tasadas.
3. **Medidas de Seguridad** y, en particular, obligaciones específicas vinculadas con la seguridad (***breach data***)
4. **Análisis de Riesgos** en el tratamiento.
5. **Evaluación de impacto** de aquellas operaciones de tratamiento que lo exijan.
6. Implantación de **la figura del Delegado de Protección de Datos** (preceptiva en las Administraciones Públicas)
7. **Códigos de conducta.**
8. **Mecanismos de certificación**
9. **Reforzamiento del papel de las autoridades de control** (AEPD/AVPD/adpCAT) en su diseño institucional, en sus funciones y en sus poderes.
10. **Régimen de responsabilidad y sanciones** (con modulaciones importantes en su aplicación a las Administraciones Públicas, de conformidad con lo que establezca la futura LOPD)

Todos y cada uno de los elementos o ejes de ese Nuevo Modelo de Gestión de Protección de Datos Personales deben ser puestos en marcha, con distinta intensidad como se decía, por todas y cada una de las Administraciones Públicas. Sin duda, el reto es importante. Y no cabe orillar que el proceso de adaptación de las estructuras organizativas de las Administraciones Públicas y de sus entidades del sector público será lento y gradual.

En verdad, **la adaptación de la gestión de protección de datos al nuevo modelo dibujado por el RGPD implicará, en primer lugar, la interiorización de cuál es la visión y sentido de esa disposición normativa (qué pretende y por qué), así como, en segundo plano, un cambio de cultura organizativa y algunas modificaciones estructurales de importancia**, como también dedicar recursos tanto personales como materiales, tecnológicos y financieros, a esa finalidad. Por ello sorprende cómo en la propia Administración General del Estado, según se recoge en el Proyecto de Ley Orgánica de

ISBN: 978-84-7777-543-3

Protección de Datos de Carácter Personal (disposición adicional undécima) se pretenda llevar a cabo ese tránsito sin coste alguno *(«(…) no podrán suponer incremento de dotaciones, ni de retribuciones, ni de otros gastos de personal»*). Mal se podrá llevar a cabo un cambio tan relevante de modelo sin afectar a estructuras, puestos de trabajo o retribuciones. Un comienzo torcido.

En cualquier caso, este Modelo de Gestión de Protección de Datos se tendrá que ir desarrollando paulatinamente, pues no cabe prever que a corto plazo de produzcan cambios sustantivos en el modo y manera de tratar los datos personales por las Administraciones Públicas. El cambio de modelo es tan radical que convendrá hacer una prudente digestión (y aplicación gradual, pero persistente) de sus innovadores elementos. Tal vez, como se dirá al final, el acelerado desarrollo de las tres oleadas de la revolución tecnológica (digitalización, automatización e Inteligencia Artificial) seguramente irán incorporado gradualmente a las Administraciones Públicas esa necesaria presión para hacer frente a tan importantes y complejos retos, que se materializarán, como expone el propio RGPD (artículo 25.1) en «los *riesgos de diversa probabilidad y gravedad* (que efectivamente se puedan ir produciendo) para los derechos y libertades de las personas físicas». También la Administración Pública y el conjunto del sector público deben impulsar de modo efectivo el desarrollo de la economía digital, pero asimismo deben salvaguardar la protección de datos personales y su adecuada utilización de conformidad con lo establecido en el RGPD. En ese justo y complejo equilibrio es en el que deberá moverse la acción de los poderes públicos.

Ni qué decir tiene que la Administración Pública que haya invertido más en ese proceso de adaptación al RGPD y sobre todo haya interiorizado su propia filosofía dispondrá de mejores recursos para poder enfrentarse a esos acelerados cambios que se advierten en un horizonte que no va más allá de los 5-10 años. Posiblemente muchas organizaciones y entidades del sector público se despierten tarde, tal como ha pasado con la implantación de las previsiones del RGPD: el 25 de mayo llegará o pasará, y el sector público seguirá teniendo retos ineludibles que cumplir en ese largo, pero necesario, camino de implantación de esa nueva concepción de defensa de los derechos fundamentales de las personas físicas a través de la protección de los datos de carácter personal. Hay, pese a que no se perciba todavía de forma generalizada, mucho en juego.

IDEA-FUERZA:

Ante la constante evolución tecnológica y los procesos de transformación digital que sufren las actividades de tratamiento de datos personales, **la reforma de la regulación de protección de datos supone un cambio del modelo tradicional para afrontar las medidas que garantizan la protección de datos personales hacia un nuevo modelo más dinámico, enfocado en la gestión continua de los riesgos potenciales asociados al tratamiento desde su diseño***»*

(AEPD*, Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*)

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_02_28-ides-idphp.php

II.

Cuestiones generales del RGPD. Algunas novedades sobre principios y derechos

1. INTRODUCCIÓN. ALGUNAS CLAVES PARA LA COMPRENSIÓN DEL RGPD

En un documento sobre la aplicación del RGPD a las Administraciones Públicas y, en especial, a las entidades locales, no puede faltar un análisis, siquiera sea epidérmico, de lo que aquí de denomina como «Cuestiones Generales», con especial atención a las novedades sobre «principios» y «derechos», algunas de ellas con particular incidencia en el quehacer cotidiano de las Administraciones Públicas cuando traten datos personales.

Todas esas normas que se recogen en los tres primeros Capítulos interesan a cualquier nivel de gobierno, sea autonómico, foral o local. Si, por ejemplo, tomamos como referencia la Administración Local, cabe subrayar que esta se caracteriza por su proximidad a la ciudadanía. Y en esta materia de protección de datos personales, las autoridades locales y sus agentes (en general es algo que debieran hacer todas las Administraciones Públicas) tendrán que llevar a cabo una labor de difusión y

ISBN: 978-84-7777-543-3

sensibilización entre la ciudadanía, complementaria a la realizada por las autoridades de control, sobre cuáles son los derechos nuevos que las personas físicas tienen, también en relación con el tratamiento de datos personales que se lleven a cabo por las organizaciones públicas. La perspectiva del ciudadano es muy importante también en este caso, en especial en Administraciones Públicas prestadoras de servicios y sobre todo (aunque no solo) cuando traten datos personales a gran escala o categorías especiales de datos.

En efecto, **no puede olvidarse nunca que el RGPD tiene por objeto la protección de las personas físicas en lo que respecta a sus derechos fundamentales y libertades públicas en su conjunto**, no solo (aunque también) se refiere al derecho a la protección de sus datos personales, sino especialmente a que a través de la lesión de este último se pueden menoscabar profundamente el ejercicio y disfrute del resto de derechos y libertades. En este punto la realidad cotidiana nos muestra que esa afectación general es cada día más real y profunda, pero especialmente —como se dirá en el Epílogo— los riesgos efectivos de que esa afectación se produzcan se incrementarán conforme avance la revolución tecnológica. Bajo ese punto de vista no es indiferente afirmar que **la protección de datos personales es, hoy en día, una batalla por el Estado democrático y por el sistema de derechos fundamentales asentados durante más de dos siglos en los países occidentales**. **Y lo será mucho más en los años venideros.**

Pero, tal como se decía, el RGPD tiene asimismo como objetivo establecer normas relativas a la libre circulación de datos que coadyuven al desarrollo de la economía digital. Algo que también se recoge en el artículo 1 del RGPD. Por consiguiente, son dos puntos de vista complementarios, si bien la protección de los datos personales y de los derechos fundamentales de las personas reúne el mayor tipo de esfuerzos reguladores del RGPD por los riesgos antes citados.

Algunas claves para la comprensión de este segundo apartado del presente trabajo se encuentran en los propios Considerandos del RGPD. Veamos sucintamente determinadas referencias y, en todo caso, se puede acudir a la lectura íntegra de los mismos para una comprensión cabal de la regulación que se examina.

¿A qué se aplican los principios de la protección de datos? (Considerando 26)*:*

— «Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable». También a los datos «seudonimizados».
— Pero no a la información anónima, entendida como aquella «que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable o deje de serlo» (Ver: artículo 2.2, a qué tratamientos no se aplica el RGPD)

Principios (Considerando 39)*:*

— «Todo tratamiento de datos debe ser *lícito y leal*».
— El principio de transparencia «exige que *toda información* y comunicación relativa al tratamiento de datos sea *fácilmente accesible y fácil de entender* y que se utilice un lenguaje sencillo y claro».
— Los *fines del tratamiento deben ser explícitos y legítimos* y determinarse en el momento de su recogida.
— Se debe *garantizar que se limiten a un mínimo estricto el plazo de conservación de los datos* (incorporar plazos para su supresión o revisión periódica).

Nuevo régimen jurídico del Consentimiento (Considerandos 32, 40 a 44)*:*

— «El consentimiento debe darse *mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca*».
— Así, a partir del RGPD, debe quedar claro que «*el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos.» (Considerando 32).*

ISBN: 978-84-7777-543-3

— Consentimiento o Base jurídica legítima: *«Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho» (Considerando 40).* Se trata de un aspecto clave, especialmente en el sector público.
— Cuando el tratamiento se lleva a cabo con el consentimiento del interesado: «*El responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación* de *tratamiento*» (véase, las exigencias en el Considerando 42).
— Asimismo, es importante tener en cuenta las *garantías del consentimiento exigidas cuando el tratamiento lo lleva a cabo una autoridad pública* (Considerando 43)

Derecho al olvido (Considerandos 65 y 66): «*Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un "derecho al olvido"*».

2. ¿CUÁL ES EL OBJETO DEL RGPD?

El objeto último es la protección de los derechos fundamentales de las personas físicas y toda la afectación que a estos derechos y libertades se pueda producir por el tratamiento de datos personales. La garantía y protección de los datos personales evita, así, que el resto de derechos y libertades de la persona física se vean «manchados» o «negados» por el efecto irradiación de los datos personales. La seguridad de los datos por parte de la «autoridad u organismo público» es consustancial, pero instrumental, para cumplir esos objetivos. Asimismo, como se viene insistiendo, no conviene perder de vista que el RGPD, en un contexto intensivo de economía digital, no puede por menos que reconocer que uno de sus objetivos es también la libre circulación de los datos personales, siempre que se cumplan determinadas exigencias establecidas en el propio Reglamento.

El artículo 1 RGPD condensa su objeto en los siguientes puntos:

— Establecer normas relativas a:

  - La protección de las personas físicas en lo que respecta al tratamiento de los datos personales.
  - La libre circulación de tales datos

— Proteger los derechos fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

PERSONAS FALLECIDAS:

También se ha de tener en cuenta que, tal como expone el Considerando 27, el RGPD «no se aplica a la protección de datos personales de personas fallecidas», siendo los Estados miembros competentes para establecer normas relativas al tratamiento de los datos personales de estas. Véase al respecto el artículo 3 («Datos de las personas fallecidas») y la Disposición adicional séptima («Acceso a contenidos de personas fallecidas») del PLOPD

3. ¿SE APLICA EL RGPD ÍNTEGRAMENTE A LAS ADMINISTRACIONES PÚBLICAS Y A SUS ENTIDADES DEL SECTOR PÚBLICO?

El RGPD es desde el 25 de mayo de 2018 norma directamente aplicable en su integridad a las Administraciones Públicas y a las entidades de su sector público (con alguna excepción puntual que se tratará: por ejemplo, la figura del delegado de protección de datos en determinadas sociedades mercantiles de capital público, al menos en la formulación actual del PLOPD, así como la problemática singular de la aplicación del régimen sancionador a las Administraciones Públicas y entidades de su sector público, entre las que no están, hoy por hoy, las sociedades mercantiles de capital enteramente público).

También se han de tener en cuenta, en un contexto globalizado y de datos abiertos, las normas que regulan las transferencias de datos personales a terceros países u organismos internacionales (Capítulo V). Esta regulación no se trata en el presente trabajo, pero debe ser siempre y en todo caso tenida en cuenta.

ISBN: 978-84-7777-543-3

IDEA-FUERZA:

«Aunque pudiera parecer que las transferencias internacionales son poco habituales en el ámbito de los entes de la Administración Local, el uso cada vez más frecuente de tecnologías de la información y la comunicación o la generalización de servicios "en nube" (*cloud computing*) supone que aumenten las posibilidades de que se trasfieran estos datos fuera del Espacio Económico Europeo dentro de los contratos de servicios informáticos».

(Ver, asimismo, artículos 45 y 46 que permiten realizar dichas transferencias internacionales sin necesidad de solicitar autorización previa a la autoridad de control)

Guía para la adaptación del Reglamento General de Protección de Datos, de las Administraciones Locales, FEMP, Grupo de Trabajo para la Implantación del nuevo RGPD en las Administraciones Locales.

Las Administraciones Públicas y las entidades de su sector público deberían haber adaptado sus protocolos, procedimientos y organización, implantado todas y cada una de las herramientas y elementos del modelo de gestión de protección de datos que se contienen en el RGPD antes de la fecha indicada (25 de mayo de 2018)

ÁMBITOS DE AFECTACIÓN DE TRATAMIENTOS EN LA ADMINISTRACIÓN LOCAL:

— Padrón Municipal
— Gestión de tributos
— Subvenciones
— *Smart Cities*

Fuente: AEPD, «Protección de Datos y Administración Local», 2018

4. EL NUEVO CONCEPTO DE «PROTECCIÓN DE DATOS» Y OTRAS DEFINICIONES

El concepto de «dato personal» se recoge en el artículo 4, 1) RGPD en los siguientes términos:

> ***«Datos personales»:*** *toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;*

Otras definiciones que, por su incidencia en la actividad local, se recomienda la consulta de su alcance en el artículo 4 RGPD:

— Tratamiento: con un amplio perímetro de lo que se considera por tal.
— Limitación del tratamiento
— Elaboración de perfiles
— Seudonimización
— Responsable del tratamiento
— Encargado del tratamiento
— Destinatario
— Violación de la seguridad de los datos personales
— Datos genéticos
— Datos biométricos

Algunas de estas definiciones serán analizadas de forma pormenorizada en otros pasajes de este texto, pero conviene tener en cuenta el alcance de tales conceptos para cualquier tarea interpretativa en la aplicación del RGPD.

> ***Datos genéticos****: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona»*

ISBN: 978-84-7777-543-3

> ***Datos biométricos:*** *«Tendrán la consideración de datos sensibles solo cuando sean utilizados para identificar unívocamente a una persona»* (AEDP, *Protección de Datos y Administración Local)*

En particular, por la importancia que tiene en el nuevo régimen jurídico de la protección de datos personales, es importante la definición de «Consentimiento del interesado» recogida en el artículo 4, 11) RGPD:

> ***«Consentimiento del interesado»:*** *toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;*

> ***¿»Interesado» o «afectado»?*** *La AEPD recomienda utilizar la expresión de «afectado» y no la de «interesado», para no incurrir en confusión con la terminología establecida en la Ley 39/2015, de 1 de octubre, de procedimiento administrativo común de las Administraciones Públicas (Protección de Datos y Administración Local)*

El PLOPD se inclina preferentemente por utilizar la noción de *afectado* más que la de interesado. Pero, en verdad, ambos términos no tienen un significado intercambiable. Por lo que respecta a la regulación recogida en el RGPD parece más adecuado seguir utilizando el término *interesado*, puesto que no siempre quien esté interesado será afectado, aunque cuando alguien sea afectado sí que será interesado.

5. ¿CUÁLES SON LOS PRINCIPIOS QUE SE DEBEN TENER EN CUENTA EN TODO TRATAMIENTO DE DATOS PERSONALES?

Los principios de protección de datos se recogen en el Capítulo II RGPD y algunos de ellos se desarrollan en el PLOPD (inexactitud de los datos, deber de confidencialidad, consentimiento afectado y de menores, etc.).

Hay que tener en cuenta que tales principio se refieren al tratamiento, por lo que son especialmente relevantes en la actuación de los responsables y encargados del tratamiento en las Administraciones Públicas. Por tanto, **el cumplimiento de tales principios interesa especialmente a la Administración Pública**. Y conviene, en consecuencia, respetar fielmente su alcance y sentido.

Los principios se pueden sistematizar partiendo de la regulación que recoge el propio artículo 5 RGPD:

— Licitud, lealtad y transparencia
— Limitación de la finalidad
— Minimización de los datos
— Exactitud
— Limitación del plazo de conservación
— Integridad y confidencialidad

Sin duda, por su por su incidencia en la actividad de las Administraciones Públicas cabe destacar, entre otros, tres de tales principios:

Limitación de la finalidad: Los datos personales serán recogidos «con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines»

UN EJEMPLO:

Según recoge la *Guía para la adaptación al RGPD de la Administración Local (FEMP)*, un posible supuesto de aplicación del principio de limitación de la finalidad de los datos sería el siguiente:

«¿Podría comunicarse por parte de un Ayuntamiento los datos de menores en situación de riesgo a una Mancomunidad que presta servicios sociales?»

Al margen de otras consideraciones generales que allí se realizan, se concluye del siguiente modo:

ISBN: 978-84-7777-543-3

«En todo caso, será preciso tener especialmente en cuenta que el RGPD regula el principio de limitación de la finalidad, es decir, que los datos no podrán ser utilizados para fines incompatibles con los fines iniciales. Por ello, **la utilización de los datos para cualquier otra finalidad distinta de la relacionada con el ejercicio de las competencias** en materia de atención a menores que tiene atribuida legalmente, **precisaría de otra legitimación específica a la luz de las normas de protección de datos de carácter personal**» (pp. 56-57)

Minimización de los datos: *Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.*

ALGÚN EJEMPLO:

Según recoge la *Guía para la adaptación al RGPD de la Administración Local (FEMP)*, algunos posibles supuestos de aplicación del principio de minimización de datos serían:

«La incorporación, tanto en la firma de los documentos electrónicos o en papel como en la marca de agua, del dato relativo al DNI del funcionario firmante, podría constituir un tratamiento excesivo y, en consecuencia, contrario al principio de minimización de datos del artículo 5 del RGPD» (p. 50)

«Con carácter general, las grabaciones indiscriminadas de voz y de conversaciones del público en general que acceden a los edificios de un Ayuntamiento a través de sistemas de videovigilancia, no cumpliría el principio de minimización de datos, considerándose una medida intrusiva» (p. 52)

Limitación del plazo de conservación: «Los datos personales serán *mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado».*

La base jurídica del tratamiento es uno de los puntos nucleares en la Administración Pública. En efecto, esta es una importante cuestión que se regula en el artículo 6 RGPD , siendo capital el apartado 1 del citado precepto (en particular, siempre que nos refiramos al sector público, los apartados a), c) y e). Muy relevante en todo caso es la previsión recogida en el artículo 6.2 RGPD, donde se recoge lo siguiente: «Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento» en determinadas circunstancias.

Licitud del tratamiento (artículo 6 RGPD: Consultar): ***El tratamiento solo será lícito si cumple (entre otras) alguna de estas condiciones****:*

- *«**El interesado dio su consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos» (letra a).*
- *«El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte» (letra b)*
- ***El tratamiento es necesario para el cumplimiento de una obligación legal** aplicable al responsable de tratamiento (letra c)*

ISBN: 978-84-7777-543-3

— ***El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos*** *conferidos al responsable del tratamiento (letra e)*
— Tratamiento para otros fines distintos de aquel para el que se recogieron los datos personales (ATENCIÓN): artículo 6.4 RGPD

IDEA-FUERZA:

Como se expone en el Considerando 26, «los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable». Por tanto, deben seguirse fielmente en toda operación de tratamiento de datos personales que lleven a cabo el responsable o el encargado del tratamiento.

EJEMPLOS. CATEGORIAS DE DATOS PERSONALES OBJETO DE TRATAMIENTO POR LA ADMINISTRACIÓN PÚBLICA:

— *De carácter identificativo* (nombre, apellidos, teléfono, DNI, imagen)
— *De carácter tributario*
— *Académicos y profesionales* (selección, bolsas, Recursos Humanos)
— *Ejercicio de potestad sancionadora*
— *Categorías especiales de datos*
— *Smart cities*

Ver: AEDP, *Protección de Datos y Administración Local.*

El PLOPD contiene algunas previsiones que conviene tener presentes:

— Disposición adicional novena. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

—Disposición adicional decimoquinta. Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.

DISPOSICIÓN ADICIONAL 9ª LOPD: **IDENTIFICACIÓN DE LOS INTERESADOS EN LAS NOTIFICACIONES POR MEDIO DE ANUNCIOS** Y PUBLICACIONES DE DATOS ADMINISTRATIVOS (SÍNTESIS)

—Acto administrativo que contiene actos de carácter personal: Identificación por nombre y apellidos, así como las cuatro últimas cifras de DNI o pasaporte.
—Notificación por medio de anuncios: Exclusivamente mediante número DNI.
—Si carece de cualquiera de los documentos anteriores: Nombre y apellidos.

6. ¿CUÁL ES LA NUEVA CONFIGURACIÓN DEL «CONSENTIMIENTO» EN EL RGPD?

Ya se ha visto la definición de consentimiento del interesado. Cuando no hay «base legal» o base jurídica específica, la Administración Pública debe solicitar inexcusablemente el consentimiento expreso e inequívoco del interesado. El artículo 6 PLOPD reenvía a la regulación del RGPD, salvo algunas precisiones (consentimiento cuando haya pluralidad de finalidades en un tratamiento). Hay una regulación particular sobre el consentimiento del niño (artículo 8 RGPD) o del menor de edad (artículo 7 PLOPD). Particular importancia tiene para la Administración Pública lo establecido en el artículo 6.1 letras c) y e) RGPD y artículo 8 LOPD, sobre tratamiento de datos amparados por la Ley (base jurídica legal).

En todo caso, se deben tener en cuenta asimismo las disposiciones adicionales decimotercera y transitoria sexta del PLOPD, que se recogen al final de este epígrafe.

En este nuevo ámbito de regulación cabe resaltar lo establecido en el artículo 7 RGPD relativo a lo que se denomina como *Condiciones para el consentimiento*. Veamos algunas de las más relevantes:

ISBN: 978-84-7777-543-3

Condiciones para el consentimiento (selección):

- —**Si el tratamiento se basa en el consentimiento del interesado**: «El responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales» (carga de la prueba del responsable)
- —**Si el consentimiento se da en un contexto de declaración escrita** que se refiera también a otros asuntos, el «consentimiento se prestará de tal forma que se distinga claramente de los demás asuntos de forma ineludible y de fácil acceso y utilizando un lenguaje claro y sencillo».
- —«El interesado tendrá **derecho a retirar su consentimiento en cualquier momento** (…) Será tan fácil retirar el consentimiento como darlo».

PROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El PLOPD recoge, asimismo, algunas disposiciones que, directa o indirectamente, pueden afectar al consentimiento.

Así, **la Disposición adicional décima («Potestad de verificación de las Administraciones Públicas»)** recoge lo siguiente:

«Cuando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos».

Por su parte, en **la «Disposición adicional decimotercera («Comunicaciones de datos por los sujetos enumerados en el artículo 77.1»)**, parece advertirse un debilitamiento de las exigencias del consentimiento según el RGPD cuando actúan entidades del sector público en determinadas circunstancias:

«Los responsables enumerados en el artículo 77.1 de esta Ley orgánica podrán comunicar los datos de carácter personal que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos o intereses de los afectados conforme a lo establecido en el artículo 6 1 f) del Reglamento (UE) 2016/679».

Pero cabe subrayar que, según el artículo 6.2 RGPD, la letra f) del citado artículo 6.1 RGPD no se aplica al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Y, en fin, la Disposición transitoria sexta («Consentimientos otorgados con anterioridad a la aplicación del Reglamento (UE) 2016/679»), expone:

«Cuando el tratamiento se base en un consentimiento otorgado con anterioridad a la aplicación del Reglamento (UE) 2016/679, no será necesario recabar nuevamente dicho consentimiento si la forma en que se otorgó se ajusta a las condiciones del Reglamento (UE) 2016/679».

UNA POSIBLE APLICACIÓN:

Por parte de alguna opinión doctrinal se ha puesto de relieve que el inciso segundo del apartado 2 del artículo 28 de la Ley 39/2015, de 1 de octubre, quedaría desplazado por el RGPD cuando afirma que «se presumirá que la consulta u obtención es autorizada por los interesados salvo que conste en el procedimiento su oposición expresa o la ley especial aplicable requiera consentimiento expreso». El problema, ciertamente, radica en que en este caso se prevé un consentimiento tácito o presunto que no se adecua, en principio, a las exigencias del RGPD.

Ver: Concepción Campos Acuña, «Los 7 imprescindibles en protección de datos para el ámbito local», *El Consultor de los Ayuntamientos y Juzgados,* enero 2018 https://bit.ly/2EftpAb

Cabe considerar que si prospera la actual redacción de la DA 10 del PLOPD, las Administraciones Públicas tendrán la potestad de verificar

ISBN: 978-84-7777-543-3

en todo caso, y sin necesidad de consentimiento, los datos que los usuarios manifiesten en las solicitudes mediante una declaración responsable. Esto supone una mejora considerable en la aplicación práctica de la simplificación de procedimientos y cumplimiento normativo de no pedir datos ni documentos a la ciudadanía que ya obren en poder de otras Administraciones Públicas. Otra cosa es que, obviamente, se requiere informar debidamente a la ciudadanía (en los términos recogidos en el RGPD) de este hecho. Habrá que esperar a cómo queda esta materia definitivamente regulada en la futura LOPD y cómo se cohonestan las previsiones del RGPD con esa finalidad de simplificación administrativa.

En todo caso, **la tesis de la AEPD es que la redacción actual del artículo 28.2 de la Ley 39/2015, podría encontrar fundamento en el artículo 6.1 e) RGPD, en concreto «cuando el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento»** (Ver: *Protección de Datos y Administración Local,* p. 13).

En el caso de la **interoperabilidad de los registros electrónicos de las Administraciones públicas,** el tratamiento podría ampararse en el cumplimiento de una obligación legal aplicable al responsable del tratamiento o, asimismo, en que ese tratamiento es necesario para el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6, 1 c) o 6,1 e) RGPD)

7. LOS TRATAMIENTOS DE «CATEGORÍAS ESPECIALES»

En los Considerandos se hace alguna mención específica a la noción «datos sensibles», pero el RGPD en su artículo 9 se refiere a la noción de «categorías especiales de datos personales», en los siguientes términos:

> *Categorías especiales de datos personales:*
>
> *9.1 RGPD: Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.*

PARA SABER MÁS:

En el tratamiento de categorías especiales de datos y las excepciones aplicables a la Administración Local, ver: AEDP, *Protección de Datos y Administración Local*, p. 14

8. ¿QUÉ DERECHOS SE GARANTIZAN POR EL RGPD AL «INTERESADO» O «AFECTADO»?

Los derechos vinculados con la protección de datos personales tienen a salvaguardar un poder de control y disposición de las personas físicas sobre tales datos, que al fin y a la postre es el contenido esencial del derecho fundamental en juego. Por consiguiente, los derechos no solo son importantes para el interesado o afectado, sino que también deben siempre tenerse en cuenta en su alcance y régimen jurídico específico por parte de las Administraciones Públicas.

El RGPD contiene una nueva regulación de los derechos de las personas en materia de protección de datos. Los viejos derechos ARCO se mantienen, se complementan o se modulan, pero se incorporan otros con perfiles nuevos, especialmente como se verá a continuación tiene particular importancia el derecho de información a los interesados o afectados, pues ha sido objeto de cambios relevantes.

Esta importante regulación está recogida en el Capítulo III («Derechos del interesado»), artículos 12 a 22. El PLOPD también prevé una regulación de tales derechos, pero salvo en los que afectan a la transparencia e información al afectado (artículo 11), derecho de acceso (artículo 13) y derecho de rectificación (artículo 14), que completan lo previsto en el Reglamento, en lo demás se lleva a cabo un simple reenvío a lo establecido en el RGPD.

Por tanto, teniendo en cuenta los fines del RGPD, las Administraciones Públicas en los procesos de tratamiento de datos tienen que adoptar medidas de carácter técnico, organizativo y de seguridad encaminadas a no afectar a ninguno de los derechos allí recogidos.

El dato siempre es de la persona, la gestión del dato cuando la ejerce una autoridad u organismo público es administrativa, pero enmarcada en el conjunto de principios, limitaciones y derechos establecidos por el RGPD.

ISBN: 978-84-7777-543-3

DERECHOS DEL INTERESADO:

- Transparencia de la información (artículos 12-13-14)
- Derecho de acceso (artículo 14)
- Derecho de rectificación (artículo 16)
- Derecho de supresión o «derecho al olvido» (artículo 17)
- Derecho a la limitación del tratamiento (artículo 18)
- Derecho a la portabilidad de los datos (artículo 20)
- Derecho de oposición y a no ser objeto de decisiones individuales automatizadas (artículos 21-22)

SI ES USTED CIUDADANO, CONOZCA SUS NUEVOS DERECHOS EN RELACIÓN CON LOS DATOS

NUEVOS DERECHOS	**ARTÍCULOS RGPD**
Derecho a recibir información clara y comprensible	(Artículos 12-14)
Derecho a solicitar acceso a los datos personas que una organización tenga sobre usted	(Artículo 15)
Derecho a solicitar a un proveedor de servicios que transmita sus datos personales a otro o se los provea	(Artículo 20)
Derecho al olvido	(Artículo 17)
Consentimiento expreso (Ya no caben extensas condiciones jurídicas que usted nunca lee)	(Artículos 4.11 y 7)
Si sus datos se pierden o son robados: Derecho a ser informado sin dilación indebida	(Artículos 33-34)
Mayor protección en línea para los menores	(Artículo 8)

[Fuente: Comisión Europea, enero 2018 (data protection-factsheet-citizens_es)]

IDEA-FUERZA SOBRE LOS DERECHOS EN EL RGPD:

— Fortalecimiento de los derechos de las personas: el Reglamento introduce nuevos requisitos de transparencia; derechos reforzados de información, acceso y eliminación («derecho al olvido»); el silencio o la falta de actividad dejarán de considerarse como un consentimiento válido, ya que se requiere una clara acción afirmativa para expresar dicho consentimiento; y la protección de los niños en línea.

(Fuente: Comunicación de la Comisión al Parlamento Europeo y al Consejo. *Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018,* Bruselas 20-1-2018 COM (2018) 43 final)

9. ¿CUÁL ES EL NUEVO MARCO NORMATIVO DE LA INFORMACIÓN Y CÓMO AFECTA A LAS ADMINISTRACIONES PÚBLICAS Y, EN PARTICULAR, A LAS ENTIDADES LOCALES?

Bajo el enunciado de «Transparencia y modalidades», los artículo 12 a 14 del RGPD contienen una nueva regulación de la Información y de las comunicaciones que se debe proveer a las personas físicas cuando se traten sus datos. Un desarrollo de tales previsiones se recoge, asimismo, en el artículo 11 del PLOPD.

El RGPD prevé, así, la Transparencia como principio (que debe ser especialmente tenido en cuenta por la Administración Pública en el ejercicio de sus funciones de tratamiento de datos) y como derecho de las personas físicas en relación con sus datos de carácter personal.

Las novedades más significativas de este nuevo marco normativo van encaminadas a reforzar la reforzar notablemente la obligación de información en todo proceso de tratamiento de datos, lo que obligará a las Administraciones Locales a tener en cuenta esas nuevas exigencias.

ISBN: 978-84-7777-543-3

Algunos rasgos de este Derecho a ser Informado son:

— El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda la información relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Esa información será tanto la indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 RGPD.

— El artículo 12.3, regula la información en relación con el ejercicio de los derechos recogidos en los artículos 15 a 22. En este caso, el responsable del tratamiento facilitará al interesado el ejercicio de sus derechos y asimismo le proveerá de la información relativa a su solicitud en el plazo de un mes o, excepcionalmente, en dos cuando se invoque complejidad o un número elevado de solicitudes. Si no da curso a su solicitud, la información será realizada sin dilación o como máximo en un mes.

— La información solicitada, tanto en uno como en otro caso, será gratuita, salvo excepciones tasadas (artículo 12.5)

— Entre la información que se debe facilitar cuando los datos se obtengan del interesado, se encuentra la siguiente:
  - Identidad y datos de contacto del responsable
  - Los datos de contacto del Delegado de Protección de Datos
  - Los fines del tratamiento a que se destinan los datos personales y la bases jurídica del tratamiento
  - El plazo en el que se conservarán los datos personales
  - La existencia del derecho a solicitar del responsable del tratamiento el acceso a los datos personales, su rectificación o supresión, la limitación del tratamiento, la oposición o la portabilidad de los datos.

— Cuando los datos no se hayan obtenido del interesado a la información anterior se le añade, la categoría de datos personales de que se trate y «la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público».

PARA SABER MÁS:

Las autoridades de control de protección de datos han elaborado conjuntamente una ***Guía para el cumplimiento del deber de informar,*** que puede consultarse en la Agencia Vasca de Protección de Datos. Ver: http://www.avpd.euskadi.eus/informacion/reglamento-general-de-proteccion-de-datos/s04-5273/es/

¿QUÉ CAMBIA EL RGPD SOBRE EL DEBER DE INFORMACIÓN EJERCIDO POR LAS ADMINISTRACIONES PÚBLICAS?

Información que cabe facilitar actualmente (LO 15/1999)	NUEVO: Información adicional que se debe añadir por aplicación del RGPD
La existencia del fichero o tratamiento	*Los datos de contacto del delegado de protección de datos*
El carácter obligatorio o no de la respuesta, así como sus consecuencias	*La base jurídica o legitimación del tratamiento*
La posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición	*La previsión de transferencias a terceros países y la existencia de una decisión de adecuación o de garantías adecuadas y los medios para obtener una copia*
La identidad y los datos de contacto del responsable de tratamiento	*El plazo o los criterios de conservación de la información*
	El derecho a solicitar la limitación del tratamiento y la portabilidad de los datos
	(*) El artículo 14.2 b) no se aplica a las autoridades y organismos públicos

ISBN: 978-84-7777-543-3

RECOMENDACIÓN DE LAS AUTORIDADES DE CONTROL SOBRE LAS OBLIGACIONES DE INFORMACIÓN DEL RGPD:

«En consecuencia, los procedimientos, modelos o formularios diseñados de conformidad con la LOPD se han de revisar y adaptar antes de la fecha de plena aplicación del RGPD, para incorporar allí los nuevos requisitos»

«Se recomienda revisar y aplicar esta adaptación sin que quepa esperar a la fecha de plena aplicación del RGPD»

Información por capas

Es preciso delimitar el Derecho a la información en una **«información por capas»**, información básica (primer nivel) y una información adicional (segundo nivel):

Presentar información básica en un primer nivel:

— de forma resumida,
— en el mismo momento y
— en el mismo medio de recogida

Remitir a información adicional en un segundo nivel:

— de forma detallada,
— en un medio más adecuado para su presentación, comprensión y archivo

RECOMENDACIÓN AEDP:

En lo que afecta al «Cumplimiento del principio de transparencia: derecho a la información en la recogida de datos personales, con la finalidad de facilitar ese cumplimiento la AEPD recomienda adoptar un modelo de información por capas o niveles. Una buena información sobre cómo llevar a cabo ese tratamiento por capas se recoge en el Cuadro de la página 28 del documento *Protección de Datos y Administración Local* editado por la AEPD. Ver Cuadro más abajo.

EJEMPLO TRATAMIENTO POR CAPAS (AEPD, *Guía de Protección de Datos y Administración Local*, abril 2018)

EPÍGRAFE	INFORMACIÓN BÁSICA (1.ª Capa resumida)	INFORMACIÓN ADICIONAL (2.ª Capa detallada)
Responsable del tratamiento	Identidad del responsable del tratamiento *(*Observación: *Dado el papel del DPD, sería recomendable incluir sus datos de contacto en la primera capa)*	1. Datos de contacto 2. Identidad/Datos contacto representante 3. Datos contacto DPD
Finalidad del tratamiento	Descripción sencilla de los fines del tratamiento, incluso elaboración perfiles	1. Descripción ampliada fines del tratamiento 2. Plazos y criterios de conservación de los datos 3. Decisiones automatizadas, perfiles y lógicas ampliadas
Legitimación del tratamiento	Base jurídica del tratamiento	1. Detalle base jurídica, en los casos de obligación legal, interés público o interés legítimo 2. Obligación o no de facilitar datos y consecuencias de no hacerlo
Destinatarios de cesiones o transferencias	Previsión o no de cesiones Previsión de transferencias o no a terceros países	Destinatarios o categorías de destinatarios Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
Derechos de las personas interesadas (o afectadas)	Referencia al ejercicio de derechos	1. Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición de su tratamiento 2. Derecho a retirar el consentimiento prestado 3. Derecho a reclamar ante la autoridad de control
Procedencia de los datos	Fuentes de los datos cuando no proceden del interesado (o afectado)	1. Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público. 2. Categorías de datos que se traten

ISBN: 978-84-7777-543-3

10. DERECHO DE ACCESO

El derecho de acceso del interesado se manifiesta en el derecho a obtener del responsable del tratamiento confirmación de si se están tratando datos personales, así como, en tal caso, el derecho de acceso a los datos y a la información recogida en el artículo 15.1 RGPD.

> ACLARACIÓN SOBRE EL DERECHO DE ACCESO RGPD:
>
> «Debe distinguirse del derecho de acceso de los interesados a los expedientes administrativos que regula la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, así como del derecho de acceso regulado en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno»
>
> *Guía para la adaptación del Reglamento General de Protección de Datos de las Administraciones Locales,* FEMP, p. 24

11. DERECHO DE RECTIFICACIÓN Y SUPRESIÓN («DERECHO AL OLVIDO»)

El interesado tiene derecho a pedir la **rectificación** de los datos personales inexactos o que no sean veraces, así como a que se completen los datos personales que estén incompletos. Esta rectificación la llevará a cabo el responsable del tratamiento, y no podrá sufrir dilaciones indebidas.

No hay novedades relevantes en lo que afecta a la rectificación de los datos, pero sí al denominado **derecho al olvido o la supresión de datos personales**, que es, sin duda, uno de los elementos nuevos de la regulación.

El responsable del tratamiento está obligado a suprimir los datos personales siempre que concurran alguna de las circunstancias establecidas en el artículo 17.1 RGPD.

En efecto, el RGPD ha sumado el «**derecho al olvido**» o derecho de supresión a los clásicos derechos ARCO —acceso, rectificación, cancelación y oposición—, pero tal «derecho al olvido» no es otra cosa que **«un derecho de cancelación actualizado».** Tanto el considerando 65 como el artículo 17 del RGPD exponen que los interesados tienen derecho al olvido si la retención de sus datos impide lo dispuesto por el propio RGPD o por la normativa del Estado miembro. Asimismo, afirma

que los interesados «deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos» o «si los interesados han retirado su consentimiento» o si se oponen al tratamiento. También indica que deberán ser suprimidos los datos personales tratados ilícitamente.

Si los datos se hacen públicos, el responsable de tratamiento deberá adoptar medidas razonables para informar a los responsables que estén tratando dichos datos, así como para suprimir cualquier enlace, copia, o réplica de los mismos, teniendo en cuenta la tecnología disponible y el coste de su aplicación.

12. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

Asimismo, el RGPD recoge expresamente el Derecho a la limitación del tratamiento (artículo 18), siempre que no concurra alguna causa legalmente prevista. Ese derecho no es absoluto, y se podrá llevar a cabo cuando se dé alguna de las siguientes condiciones:

- Se podrá limitar el tratamiento de los datos del interesado cuando este haya impugnado su exactitud, durante el plazo que el responsable los verifique.
- Si el tratamiento es ilícito, el interesado podrá pedir la limitación del uso de los datos en vez de su supresión.
- Cuando el responsable ya no necesite hacer uso de esos datos, pero el interesado los necesite para interponer o defender reclamaciones.
- Cuando el interesado se haya opuesto al tratamiento de sus datos por motivos relacionados con su situación particular, mientras se verifica si los motivos han de tenerse en cuenta.

13. DERECHO A LA PORTABILIDAD DE LOS DATOS

El derecho a la **portabilidad de los datos** supone el «derecho del interesado a recibir su información en un formato estructurado y de uso común, para su trasmisión a otro responsable o, incluso la obligación del anterior responsable de hacerlo directamente», esto último será posible cuando sea técnicamente viable. El derecho a la portabilidad de los datos personales está directamente relacionado también con la libre circulación de tales datos.

ISBN: 978-84-7777-543-3

> —Mayor control sobre los datos personales para los particulares. El Reglamento establece un **nuevo derecho a la portabilidad de los datos** que permite a los ciudadanos solicitar que una empresa u organización le devuelva los datos personales que le facilitó por consentimiento o contrato; también permitirá que dichos datos personales se transmitan directamente a otra empresa u organización, cuando sea técnicamente posible.
>
> *(Fuente:* Comunicación de la Comisión al Parlamento Europeo y al Consejo. *Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018,* Bruselas 20-1-2018 COM (2018) 43 final)

Esquema de Ideas-Fuerza

- El artículo 20 RGPD crea un nuevo derecho a la portabilidad de los datos estrechamente relacionado con el derecho de acceso aunque diferente de este en muchos aspectos. Ciertamente, tanto en los derechos nuevos como en los existentes anteriormente se produce en ocasiones una suerte de «encabalgamiento» de derechos que pueden llegar a ofrecer en algunos momentos dificultades de deslinde.
- El propósito de este nuevo derecho es capacitar al interesado y darle más control sobre los datos personales que le conciernen.
- El derecho a la portabilidad de los datos es también una herramienta importante que respaldará la libre circulación de datos personales en la UE y facilitará el cambio entre distintos proveedores de servicios y, por tanto, promoverá el desarrollo de nuevos servicios en el contexto de la estrategia para el mercado digital.
- Una práctica recomendable es que los responsables del tratamiento comiencen a desarrollar los medios que contribuyan a responder a las solicitudes de portabilidad.

PARA SABER MÁS:

Grupo de Trabajo sobre Protección de Datos del Artículo 29: *Directrices sobre el derecho a la portabilidad de los datos,* 16/ ES, WP 242 rev. 01 (Adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017)

Se puede consultar en la página Web de la AVPD: http://www.avpd.euskadi.eus/informacion/reglamento-general-de-proteccion-de-datos/s04-5273/es/, en la pestaña «Directrices de la autoridades europeas para facilitar el cumplimiento y aplicación del Reglamento»

14. DERECHO DE OPOSICIÓN Y DECISIONES INDIVIDUALES AUTOMATIZADAS

El interesado podrá, siempre que no concurra alguna de las excepciones previstas en el Reglamento, **oponerse** a que sus datos sean objeto de tratamiento. Esta oposición se podrá presentar en cualquier momento, y se podrá basar en motivos relacionados con la situación particular del interesado. Si se presenta la oposición, el responsable del tratamiento deberá dejar de tratar los datos personales.

15. LIMITACIONES

Los derechos mencionados no son absolutos, sino que se pueden encontrar limitados por varios factores.

El responsable o el encargado del tratamiento, siempre que encuentre cobertura tal limitación en el Derecho de la Unión o de los Estado miembros a través de medidas legislativas, podrá limitar dichos derechos, siempre y cuando las medidas adoptadas sean necesarias y proporcionadas y respete lo previsto en la normativa para ello, asimismo la limitación deberá siempre respetar en lo esencial los derechos y libertades fundamentales.

El artículo 23 del RGPD dispone los casos en los que se acepta la limitación de los derechos del interesado, atendiendo, siempre, a la necesidad de salvaguardar, entre otros, la defensa, la prevención, investigación o enjuiciamiento de infracciones penales, la seguridad pública, la protección del interesado o de los derechos y libertades de otros.

ISBN: 978-84-7777-543-3

ADVERTENCIA:

Debe ponerse de relieve que el actual artículo 7.5 de la LOPD de 1999, establece lo siguiente:

> *«5. Los datos de carácter personal relativos a la comisión de* ***infracciones penales o administrativas*** *sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.»*

Mientras que el artículo 23.1 d), relativo a las limitaciones «a través de medidas legislativas» de los Estados miembros, expone:

> *«d) La prevención, investigación, detección o enjuiciamiento de* ***infracciones penales*** *o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención»*

Por tanto, se ha acortado el perímetro de la limitación y no se incluyen a las infracciones administrativas, lo que podría tener consecuencias, también en lo que, en su caso, afecte a la transparencia y al derecho de acceso a la información pública (por ejemplo, artículo 14.1 e) Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno).

III.

Nuevo Sistema institucional y de gestión de protección de datos en la Administración Pública

1. INTRODUCCIÓN

El nuevo modelo de Protección de Datos que se prevé en el RGPD se asienta, tal como se viene reiterando, sobre la ***responsabilidad proactiva***, lo que tiene especiales consecuencias a la hora de articular el sistema institucional y de gestión de protección de datos en las Administraciones Públicas. Efectivamente, ese cambio de paradigma obliga a las organizaciones del sector público a *construir* un modelo de gestión que dé respuesta cabal a los hipotéticos riesgos que se puedan producir en un futuro inmediato o mediato, objetivo para el cual se debe repensar gradualmente el modelo organizativo y recomponer las piezas que sean necesarias para que este se articule efectivamente en la orientación y finalidad del RGPD.

ISBN: 978-84-7777-543-3

Se pone, por tanto, el acento principalmente en hacer frente a «los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas» (artículo 24.1 RGPD) y, por tanto, en la adopción de determinadas medidas tales como, entre otras, la protección desde el diseño y por defecto, el análisis de riesgos y la evaluación de impacto que conlleva determinados tratamientos de datos personales, así como la adopción de códigos de conducta y mecanismos de certificación; es decir, **el foco se sitúa en la anticipación y en la prevención, una suerte de garantía y aplicación de la política de cumplimiento (*compliance*) también en las organizaciones públicas**.

Ni que decir tiene que **este enfoque de riesgos y preventivo implica un cambio de cultura organizativa frontal en lo que al tratamiento de datos respecta.** Al menos impone una forma distinta de trabajar en todos los procesos, procedimientos y proyectos que impliquen tratar datos de forma masiva, que entrañen alto riesgo y aquellos otros que se encuadran en «categorías especiales» (datos sensibles). También supone articular de modo efectivo todas las piezas de ese nuevo modelo institucional y de gestión en las distintas organizaciones públicas, aspecto sobre el que se deberá trabajar de forma especial en los próximos tiempos, pues —tal como se dice en el Epílogo— la revolución tecnológica está inmersa en un proceso de aceleración e innovación disruptiva (Schumpeter) y la protección de datos de las personas físicas es un bien a proteger especialmente por lo que a la afectación a los derechos fundamentales respecta.

Y es aquí donde se hallan los principales problemas para transitar correctamente de un modelo de protección de datos «reactivo» a otro «proactivo». La formación se torna ineludible y las políticas de sensibilización, así como las distintas Guías y materiales que elaboran y ponen en marcha estas autoridades de control (AVPD/apdCAT/AEPD), junto con las administraciones públicas, son una herramienta o palanca de cambio o transformación imprescindible para ir introduciendo paulatinamente la **nueva cultura de gestión en la protección de datos personales.**

El tránsito será lento, también en el sector público. Se ha comenzado tarde y habrá que ajustar paulatinamente los distintos elementos de esa nueva arquitectura institucional y de gestión que deberá funcionar en un plazo razonable de forma armónica, sobre todo si, según se decía, se quiere que los datos personales y los derechos fundamentales de las personas físicas no sufran menoscabo alguno.

De hecho, ese nuevo sistema de gestión debiera estar ya listo para funcionar con anterioridad al 25 de mayo de 2018, pero su puesta en

marcha en el sector público se dilatará en el tiempo, al menos en algunos casos. En cualquier caso, no hay excusa, puesto que el RGPD se aprobó con un largo periodo que difería su aplicabilidad precisamente para garantizar su efectividad y llevar a cabo tal proceso de adaptación.

Y, para articular razonablemente, las diferentes piezas que gravitan en torno a la construcción de ese nuevo modelo institucional y de gestión de la protección de datos personales en el sector público, se deben tener presentes, aparte de los principios y derechos antes recogidos, una serie de elementos organizativos e institucionales que tienden a configurar un nuevo Sistema de Gestión de la Protección de Datos en el Sector Público que se configura de los siguientes elementos básicos:

Elementos Básicos del Sistema de Gestión de Protección de Datos	Ubicación sistemática en el RGPD
Responsables/Encargados del tratamiento	Capítulo IV RGPD (artículos 24-29)
Registro de las Actividades de tratamiento	Artículo 30 RGPD
Seguridad de los datos personales	Artículos 32-34 RGPD
Análisis de Riesgos	Proceso previo, en su caso, a la evaluación de impacto
Evaluación de impacto relativa a la protección de datos	Artículos 35-36
Delegado de Protección de Datos	Artículos 37-39
Códigos de Conducta	Artículos 40-41
Mecanismos de Certificación	Artículos 42-43
Autoridades de Control (AEPD/ACPD)	Artículos 51-59 (especialmente) Título VII PLOPD
Régimen de Sanciones	Capítulo VIII RGPD Título IX PLOPD

El objeto, por tanto, de esta tercera parte de la Guía no es otro que analizar brevemente y de forma descriptiva estos elementos que configuran la arquitectura básica del Sistema Institucional y

ISBN: 978-84-7777-543-3

de Gestión de la Protección de Datos en las organizaciones públicas, con la finalidad de que este análisis sirva como medio de activar la puesta en marcha de todas esas piezas de este complejo engranaje a la mayor brevedad por parte de las Administraciones Públicas y de sus entidades del sector público institucional, pero especialmente de las Administraciones locales que son el objeto central de estas líneas.

En cualquier caso, tiempo habrá de profundizar en todos y cada uno de los elementos citados (en algún caso, como es la figura del Delegado de Protección de Datos, ya lo hemos hecho en un trabajo previo; véase: http://laadministracionaldia.inap.es/noticia.asp?id=1508368). Sin duda, el análisis puntual de todos y cada uno de los elementos citados deberá esperar, asimismo, a que la futura LOPD vea la luz y se concreten algunas de las cuestiones en las que el RGPD deba recibir un complemento o desarrollo por la legislación de los Estados miembros.

2. RESPONSABLES DE TRATAMIENTO Y ENCARGADOS DE TRATAMIENTO: SUS PECULIARIDADES APLICATIVAS EN EL ÁMBITO DEL GOBIERNO LOCAL

Responsable de tratamiento

El Considerando 78 RGPD comienza del siguiente modo: «La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento».

La puesta en marcha de esas medidas técnicas y organizativas apropiadas es una responsabilidad de una figura clave en el modelo de protección de datos, también en el sector público: el responsable del tratamiento. Junto a esta figura también se encuentra otra que es la del «encargado del tratamiento» (que ha sido objeto de algunas modificaciones importantes en su régimen jurídico, tal como se verá), ambas deben estar condiciones de cumplir sus obligaciones en materia de protección de datos. Y, además, implantar los principios de protección de datos desde el diseño y por defecto. Este último aspecto es, sin duda, determinante del nuevo modelo, que se asienta en la prevención de riesgos en los tratamientos de datos de carácter personal actuales y futuros.

Dos Considerandos son importantes en esta materia. Y conviene reproducirlos para poder extraer sus consecuencias efectivas:

CONSIDERANDO 79:

«La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable».

CONSIDERANDO 81:

«Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a 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 adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del

ISBN: 978-84-7777-543-3

interesado (…) Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos.»

La figura del responsable de tratamiento viene definida en el artículo 4.7 RGPD en los siguientes términos:

«"RESPONSABLE DE TRATAMIENTO" O "RESPONSABLE": La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros determine los fines y medios del tratamiento (…)»

La regulación específica de la figura del responsable de tratamiento se halla en los artículos 24 a 27 RGPD, si bien el Reglamento está plagado de referencias permanentes a esta figura, que se transforma así en pieza clave para garantizar el perfecto cumplimiento de las obligaciones derivadas de la norma europea o del Derecho interno de los Estados miembros, así como en garante último de que se adoptarán las medidas técnicas y organizativas apropiadas para su adecuación a tal normativa.

Esta idea se refleja perfectamente en el artículo 24 RGPD, cuyo apartado 1 expone, por ejemplo, lo siguiente:

«Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento ***así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento.*** *Dichas medidas se revisarán y actualizarán cuando sea necesario.»*

Por tanto, la aplicación de las medidas técnicas y organizativas que debe poner en marcha quien ejerza las funciones de responsable del tratamiento dependerán de la naturaleza, contexto y fines del tratamiento, pero especialmente (y aquí viene la dimensión preventiva articulada con la evolución futura de este problema) teniendo en cuenta ***los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas.*** Tal como expresa el artículo 24.3 RGPD la adhesión a códigos de conducta o mecanismos de certificación «podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento».

El artículo 25 RGPD, por su parte, recoge una de las ideas sustantivas del nuevo modelo centrado específicamente en la gestión de riesgos, algo que se tratará en el epígrafe de este documento relativo al Análisis de Riesgos, pero conviene reproducir, por su importancia implícita, los apartados 1 y 2 del citado precepto. Como puede advertirse la protección de datos desde el diseño y por defecto es responsabilidad exclusiva del propio responsable del tratamiento, que deberá asimismo aplicar las medidas técnicas y organizativas apropiadas teniendo en cuenta lo establecido en el primer inciso de ese mismo precepto.

Artículo 25.1 Y 2 RGPD: PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

*«1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, **el responsable del tratamiento aplicará**, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, **medidas técnicas y organizativas apropiadas**, como la seudonimización, concebidas **para** aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y **proteger los derechos de los interesados.»***

ISBN: 978-84-7777-543-3

> *«2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.»*

El artículo 26 regula la figura del corresponsable («cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento») y el régimen aplicable (por ejemplo, «los corresponsables determinarán de modo más trasparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento»).

El PLOPD, por su parte, establece una minuciosa regulación en su Título V del responsable y encargado del tratamiento. Sin perjuicio de cómo quede finalmente esa regulación en el texto que definitivamente se apruebe, algunos de los puntos que allí se tratan en relación con el papel del responsable son los siguientes:

- Con el fin de concretar las medidas técnicas y organizativas que los responsables y encargados han de adoptar, se determinan una serie de supuestos en los que se podrían producir «mayores riesgos», lo que puede ayudar a definir en qué casos se pueden adoptar tales medidas (artículo 28.2 PLOPD)
- El artículo 31 PLOPD regula el Registro de actividades de tratamiento y, entre otras cosas, establece la necesidad de comunicar por parte del responsable o del encargado del tratamiento al Delegado de Protección de Datos «cualquier adición, modificación o exclusión del contenido del registro»
- También en ese mismo artículo 31.2 PLOPD se establece la obligación de que las Administraciones Públicas y sus entidades del sector público (recogidas en el ámbito de aplicación del artículo 77.1 PLOPD) hagan público un inventario de actividades de tratamiento.

— Se fija la obligación del responsable del tratamiento de «bloquear los datos cuando proceda a su rectificación o supresión», así como se regula a disposición de qué autoridad quedan tales datos. También se indica que «los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior» (artículo 32, 1 a 3). El apartado 4 prevé un régimen de excepciones que pueden definirse por las autoridades de control en los términos allí previstos.

En el ámbito local de gobierno la figura del responsable de tratamiento será habitualmente el Alcalde o Alcaldesa, salvo que tal atribución haya podido ser delegada en un miembro de su equipo de Gobierno o, asimismo, en la persona titular de un órgano directivo en los municipios de gran población. Esta atribución de responsabilidades en una persona de extracción política exige en el nuevo modelo adaptar todas y cada una de las piezas que se configuran con la finalidad de salvaguardar no solo los derechos fundamentales de las personas físicas, sino en este caso también proteger adecuadamente que se puedan derivar responsabilidades hacia miembros del equipo de gobierno. Lo mismo se podría decir de aquellas Administraciones (Administración Vasca o Administraciones Forales) que hagan descansar la figura del responsable de protección de datos en órganos superiores o directivos que se provean exclusivamente por criterios de nombramiento político.

PARA SABER MÁS:

En relación con el trascendental papel de la figura del Responsable de tratamiento, también en las Administraciones Públicas, es de gran interés la ***Guía del Reglamento General de Protección de Datos para responsables de tratamiento.***

Ver el documento en PDF en la página de la Agencia Vasca de Protección de Datos:

http://www.avpd.euskadi.eus/informacion/reglamento-general-de-proteccion-de-datos/s04-5273/es/

ISBN: 978-84-7777-543-3

UNA PROPUESTA:

En todo caso, atendiendo a la importancia estratégica o nuclear que tiene la figura del responsable en la aplicación efectiva del nuevo modelo de gestión del RGPD, cabría plantearse la oportunidad de elaborar en las Administraciones Públicas, y asimismo al menos en determinadas entidades locales de ciertas dimensiones, una normativa reglamentaria de corte organizativo que regule estas cuestiones. Por ejemplo, en el ámbito local esta normativa podría ser el Reglamento Orgánico Municipal o una disposición normativa reglamentaria de Protección de Datos que, con un evidente carácter organizativo, determinara no solo el papel del responsable o responsables en la estructura municipal en materia de protección de datos, sino también sus relaciones con la figura del encargado o encargados de tratamiento, así como en relación con el Delegado de Protección de Datos (y la definición concreta de esa figura en la organización), pudiendo igualmente regular otros aspectos específicos de tal materia (Seguridad, Registro de Actividades, Análisis de Riesgos, Evaluación de Impacto, etc.). Todos estos aspectos también podrían regularse, según se decía, en las Administraciones autonómicas y forales, lo que daría mayor empaque al modelo y aportaría seguridad jurídica a la hora de determinar las responsabilidades de cada actor en estos procesos de tratamiento de datos personales.

También cabría plantearse si toda esta información y la organización no se pueden seguir reflejando en el Documento de Seguridad, dado que se podría considerar vigente en cuanto que no contradice lo previsto en el RGPD. En cualquier caso, el cambio de paradigma es tan profundo (al menos en sus finalidades y arquitectura institucional) que tal vez requiera plantearse (siquiera sea como mera hipótesis) un reflejo normativo, como antes se indicaba.

PARA SABER MÁS

Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento, AEPC, AVPD, apdCAT, 2018.

http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf

Encargado de protección de datos

Ya se ha visto cómo el Considerando 97 delimita a rasgos generales cuál es el papel y perfil que debe tener esta figura. Su regulación en el RGPD se encuentra recogida en los artículo 28 y 29, principalmente en el primero que resulta fundamental para concretar los criterios generales expuestos en el Considerando 97 sobre cuál es el régimen aplicable a la figura del encargado de tratamiento.

Dada la finalidad del RGPD de protección de los datos de carácter personal y, concretamente, de los derechos fundamentales de las personas físicas que se puedan ver afectados por tales tratamiento de datos, la norma europea introduce algunas novedades importantes en la regulación del encargado del tratamiento, con el objetivo de apuntalar el cumplimiento estricto del propio Reglamento, puesto que en las Administraciones Públicas tales datos en unas ocasiones serán tratados por encargados «internos», pero en no pocas de ellas por encargados «externos», mediante procedimientos de contratación pública, encomiendas de gestión, convenios u otros instrumentos jurídicos.

De ahí que la regulación de esta figura se prevea con cierto detalle. Y de ahí también cómo las autoridades de control (AEPD/apdCAT/AVPD) han elaborado, según se verá de inmediato, un documento de notable interés sobre el encargado del tratamiento y, asimismo, sobre el papel del responsable de tratamiento en relación con aquel.

> PARA SABER MÁS:
>
> *«Directrices para la elaboración de contratos entre responsables y encargados de tratamiento»*.
>
> *Ver*: http://www.avpd.euskadi.eus/informacion/reglamento-general-de-proteccion-de-datos/s04-5273/es/

La regulación sustantiva de esa figura se lleva a cabo en el artículo 28 RGPD, del que se pueden destacar los siguientes aspectos:

— El apartado 1 expone lo siguiente: «Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, éste elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.»

ISBN: 978-84-7777-543-3

— En el apartado 2 se regula que **el encargado del tratamiento no podrá recurrir a otro encargado sin la autorización previa por escrito, específica o general, del responsable**. Debiendo informar de todo cambio.
— **El tratamiento por el encargado se regirá por un contrato o acto jurídico**, que deberá estipular, en particular, una serie de exigencias que se detallan en el artículo 28.3 RGPD.
— Cuando un encargado recurra a otro para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se le impondrán, también por contrato o acto jurídico, las mismas obligaciones de protección de datos estipuladas en el contrato o acto jurídico existentes entre el responsable y encargado principal (artículo 28.4)
— **La adhesión a códigos de conducta o mecanismos de certificación podrá utilizarse** como elemento para demostrar que se cumplen las garantías establecidas en ese artículo 28.1 a 4.
— Se prevé una referencia a las cláusulas contractuales tipo y a la facultad de adoptarlas por la Comisión o por la autoridad de control.
— Se contiene asimismo la exigencia de que el contrato u otro acto jurídico sea siempre por escrito (formato electrónico, actualmente).
— **Y, en fin, se incorpora una importante cláusula de desplazamiento de la responsabilidad en determinados supuestos** (artículo 28.10).

El PLOPD contiene en su artículo 33 una regulación de la figura del encargado del tratamiento, cuyas notas más relevantes, sin perjuicio de cómo quede finalmente en el texto de la Ley Orgánica que se apruebe, son las siguientes:

— «El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos», si se cumple lo establecido en la normativa de aplicación.
— Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 RGPD. Se exceptúan de esta regla los encar-

gos efectuados en el marco de la legislación de contratación del sector público.

— «Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades».

— El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos de carácter personal deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. Se establece alguna excepción.

— «El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento».

— «En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679».

DISPOSICIÓN TRANSITORIA QUINTA PLOPD. CONTRATOS DE ENCARGADOS DEL TRATAMIENTO

«Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y, en caso de haberse pactado de forma indefinida, hasta transcurridos cuatro años desde la citada fecha.

En caso de que los contratos previesen su prórroga al término de su vencimiento, ya fuera por mutuo acuerdo entre las partes o en ausencia de denuncia por cualquiera de ellas, deberá producirse su adaptación con anterioridad al momento en que estuviera prevista dicha prórroga.»

ISBN: 978-84-7777-543-3

Y, en fin, para tener una idea más cabal del papel y de las novedades que implica la figura del Encargado del tratamiento, así como de sus relaciones con el Responsable del tratamiento, debe consultarse el importante Documento de Directrices para la elaboración de contratos entre responsables y encargados del tratamiento, difundido por la AVPD con el título ya indicado, que es el que se utilizará como referencia en este texto.

IDEAS-FUERZA de las *«Directrices para la elaboración de contratos entre responsables y encargados de tratamiento»*. AEPD-AVPD-apdCAT

¿QUÉ ES UN ENCARGADO DEL TRATAMIENTO Y CUÁL ES SU FUNCIÓN PRINCIPAL?

- El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u organismo que presta al responsable un servicio que conlleva el tratamiento de datos personales por cuenta de éste.
- Aunque la definición puede parecer clara, en la práctica se dan multitud de situaciones en las que puede ser difícil delimitar cuándo nos encontramos ante un encargado y en qué casos ante un responsable del tratamiento. Para facilitar esta distinción, debemos tener en cuenta que **corresponde al responsable decidir sobre la finalidad y los usos de la información, mientras que el encargado del tratamiento debe cumplir las instrucciones de quien le encomienda un determinado servicio, en relación con el tratamiento de los datos personales a los que tiene acceso como consecuencia de la prestación de este servicio**.

¿QUÉ NIVEL DE DECISIÓN PUEDE ASUMIR UN ENCARGADO DEL TRATAMIENTO?

—El encargado del tratamiento puede adoptar cualquier decisión organizativa y operacional necesaria para prestar el servicio que tiene contratado. En ningún caso puede variar los fines y los usos de los datos, ni puede utilizarlas para sus propias finalidades.
—Las decisiones que adopta deben respetar las instrucciones del responsable del tratamiento.

¿EL RESPONSABLE DEL TRATAMIENTO PUEDE ELEGIR CUALQUIER ENCARGADO DEL TRATAMIENTO?

—El responsable del tratamiento debe elegir un encargado del tratamiento que ofrezca garantías suficientes respecto de la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas. Por lo tanto, hay un deber de diligencia a la hora de escoger el encargado.
—La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, incluido en formato electrónico.

¿CÓMO REGULAR LAS RELACIONES ENTRE EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO?

—La posibilidad de regular esta relación a través de un acto jurídico unilateral del responsable del tratamiento es una de las novedades previstas en el RGPD. En cualquier caso, debe ser un acto jurídico que establezca y defina la posición de el encargado del tratamiento, siempre que dicho acto vincule jurídicamente el encargado del tratamiento. Este sería el caso, por ejemplo, de una resolución administrativa que conste notificada al encargado del tratamiento.

ISBN: 978-84-7777-543-3

¿QUIÉN ES RESPONSABLE DE LOS TRATAMIENTOS REALIZADOS POR EL ENCARGADO DEL TRATAMIENTO?

— El responsable del tratamiento no pierde esta consideración ningún caso. Por tanto, sigue siendo responsable de que los datos personales se traten correctamente y de la garantía de los derechos de las personas afectadas.
— El responsable tiene una obligación de especial diligencia en la elección y la supervisión de el encargado

SI SE EXTERNALIZAN LAS FUNCIONES DEL DELEGADO DE PROTECCIÓN DE DATOS A UN TERCERO, ESTE TIENE LA CONSIDERACION DE ENCARGADO DEL TRATAMIENTO?

— Sí, el RGPD prevé que el delegado de protección de datos debe poder acceder a los datos que se traten. Por lo tanto, se deberá formalizar un encargo del tratamiento.

¿CUAL ES EL CONTENIDO MÍNIMO DE UN ACUERDO O ACTO DE ENCARGO DEL TRATAMIENTO? (VER LA DESCRIPCIÓN DE CADA PUNTO LA GUÍA)

— Las instrucciones del responsable del tratamiento.
— El deber de confidencialidad
— Las medidas de seguridad
— El régimen de la subcontratación
— Los derechos de los interesados
— Colaboración en el cumplimiento de las obligaciones del responsable
— El destino de los datos al finalizar la prestación
— La colaboraciones para demostrar el cumplimiento

ENCARGADO DE TRATAMIENTO: EJEMPLOS CUANDO UN AYUNTAMIENTO ENCARGA A UN TERCERO EL TRATAMIENTO DE DATOS

- Elaboración de nóminas de personal
- Destrucción de documentación
- Control de cámaras videovigilancia
- Gestión de cobro de impuestos
- Mantenimiento de equipos informáticos

Fuente: AEPD, *Protección de Datos y Administración Local*

3. REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO

Se trata, sin duda, de una de las novedades más significativas del RGPD, que enlaza directamente con la filosofía que impregna el nuevo modelo de gestión de datos personales.

La creación u mantenimiento de un registro de actividades de tratamiento es una obligación que deben llevar a cabo necesariamente los responsables del tratamiento (o sus representantes) y los encargados del tratamiento (o sus representantes). Y sustituye la antigua obligación de notificar los ficheros y tratamientos a las autoridades de control (AVPD, en el caso de la Comunidad Autónoma del País Vasco). No es un registro de ficheros, sino de tratamientos.

HERRAMIENTAS. CÓMO IMPLANTAR EL REGISTRO DE ACTIVIDADES: Un buen modelo de Registro de actividades de tratamiento, a partir del «ciclo de vida de los datos», puede hallarse en: *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*, pp. 36-39

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

ISBN: 978-84-7777-543-3

El marco regulatorio viene establecido por el artículo 30 RGPD

Aunque cabe tener en cuenta lo que al respecto establezca la futura LOPD (artículo 31 PLOPD). Las Administraciones Públicas y sus entidades del sector público institucional (con excepción de las sociedades mercantiles públicas) «harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos» (artículo 31.2 PLOPD).

Hay que tener en cuenta que estos Registros de Actividades de tratamiento del Responsable o del Encargado tienen distinta intensidad en cuanto a su contenido, tal como establecen los apartados 1 (Responsable) o 2 (Encargado) del artículo 30 RGPD:

Responsables de tratamiento	Encargados de tratamiento
Nombre y datos de contacto del responsable o de su representante	Nombre y datos de contacto del encargado o de su representante
Nombre y datos de contacto del DPD	Nombre y datos de contacto del DPD
Fines del tratamiento	Categorías de tratamientos
Categorías interesados y de datos personales	
Categorías destinatarios comunicaciones, incluidos destinatarios terceros países	
Transferencias internacionales tercer país	Transferencias internacionales tercer país
Plazos previstos supresión categorías datos	
Medidas técnicas y organizativas de seguridad: descripción general	Medidas técnicas y organizativas de seguridad: descripción general

El artículo 30.5 RGPD expone lo siguiente:

> *«Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas*

en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10».

No obstante, este precepto se ha de interpretar de conformidad con lo establecido en el Considerando 13 «in fine». Su aplicabilidad como excepción a las Administraciones Públicas y, en particular, a las Administraciones locales o entidades del sector público, se ha de enmarcar en tales exigencias. Por los datos que se tratan en el ámbito local, al menos en algunos casos, la excepción entendida como inaplicación parece que no operaría en este caso.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO ADMINISTRACIÓN LOCAL: ALGUNOS EJEMPLOS:

- Impuesto vehículos: «Por ejemplo, si los datos que se utilizan para el cobro del impuesto de vehículos se usan para informar sobre una campaña informativa sobre contaminación producida por los citados vehículos, existirán dos tratamientos de esos datos: uno respecto al cobro del impuesto y otro referente a la citada campaña» (pp. 15-16)
- Registro de actividades del Padrón Municipal y de Seguridad, ver: pp. 17-18

Fuente: AEPD, *Protección de Datos y Administración Local*

4. SEGURIDAD DE LOS DATOS PERSONALES

En el RGPD la seguridad se vincula estrechamente con la protección de datos personales y con la salvaguarda de los derechos y libertades de las personas físicas. Este es un enfoque de seguridad diferente, pues tiende a formar parte de ese Sistema de Gestión de Datos Personales que deben activar todas las organizaciones públicas.

Las novedades que introduce el RGPD en este ámbito también son importantes, sobre todo por la naturaleza proactiva de los tratamientos y la necesidad de tener el enfoque de riesgos estrechamente vinculado con los sistemas de seguridad. Ello imprime un concepto de seguri-

ISBN: 978-84-7777-543-3

dad «dinámico» o «instantáneo», que depende del responsable del tratamiento. Este concepto de seguridad se debe enmarcar necesariamente en un contexto de revolución tecnológica que tendrá impactos potencialmente muy fuertes sobre el ámbito de los datos personales (Ver Epílogo).

El marco regulatorio es muy preciso: Artículos 32 y 33 del RGPD. Ver asimismo la Disposición Adicional primera del PLOPD. En esta última referencia se emplaza a una modificación del Esquema Nacional de Seguridad para adaptarlo a las exigencias del RGPD, lo que implicará la modificación o adaptación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

> Disposición Adicional Primera PLOPD:
>
> *«El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos de carácter personal para evitar su pérdida, alteración o acceso no autorizado, adaptando criterios de determinación del riesgo en el tratamiento de los datos en el artículo 32 del Reglamento (UE) 2016/679»*

En función de una serie de variables que se enuncian en el artículo 32.1 RGPD, «el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo», que incluya, entre otras cuestiones:

- Seudonimización y cifrado de datos personales.
- Garantía de confidencialidad, integridad, disponibilidad y resiliencia de los sistemas.
- Capacidad de restaurar la disponibilidad y acceso rápidamente en casos de incidentes.
- Verificación, evaluación y valoración con carácter regular de la eficacia de las medidas técnicas y organizativas (*) (**).

(*) Cuando se evalúe la adecuación del nivel de seguridad se tendrán en cuenta los riesgos (algo que se trata en el siguiente epígrafe).

(**) La adhesión a códigos de conducta y mecanismos de certificación pueden servir como medios de cumplimiento de los requisitos establecidos.

IMPORTANTE PARA LA ADMINISTRACIÓN PÚBLICA Y ENTIDADES VINCULADAS, ASÍ COMO PARA LOS EMPLEADOS PÚBLICOS :

«El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable (…)» (Artículo 32.4 RGPD).

IDEAS-FUERZA SOBRE MEDIDAS SEGURIDAD SEGÚN LA AEPD:

- «El RGPD no establece medidas de seguridad estáticas, por lo que corresponderá al responsable determinar aquellas medidas de seguridad que sean necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales» (p. 20).
- «En ningún caso el RGPD se debe entender como la eliminación automática de tales medidas de seguridad ya existentes» (p. 20).
- «La seudonimización contribuye a reducir riesgos»

(AEPD, *Protección de Datos y Administración Local*

Data Breach: violaciones del sistema de seguridad

Se trata también de una importante novedad del RGPD. Se regula en los artículos 33 y 34, ofreciendo un doble régimen jurídico de notificación o comunicación inmediata («sin dilación indebida») por parte del responsable del tratamiento a la autoridad de control y a los interesados, respectivamente, en los casos de violación de seguridad que comporten pérdida, alteración o destrucción de datos.

Hay, por tanto, una obligación institucional doble y está detrás de esta regulación asimismo un *derecho de la persona física a ser informado de las violaciones del sistema de seguridad que entrañen alto riesgo para los derechos y libertades de las personas físicas*. El encargado lo debe poner de inmediato en conocimiento del responsable.

ISBN: 978-84-7777-543-3

Régimen de notificaciones y comunicaciones:

—A la autoridad de control. Requisitos:

- A más tardar 72 horas después de que se haya tenido constancia de la violación.
- No es necesaria cuando sea improbable un riesgo para los derechos y libertades de la persona.
- La notificación debe recoger una serie de exigencias establecidas en el artículo 33.3 RGPD.
- La autoridad de control verifica el cumplimiento de lo previsto en el artículo 33 RGPD.

—A los interesados. Requisitos:

- Se comunica la violación de los datos personales «cuando sea probable que entrañe un alto riesgo para los derechos y libertades».
- La comunicación describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad, así como deberá cumplir determinadas exigencias (artículo 34.2 RGPD).
- Supuestos en que no es necesaria (artículo 34.3 RGPD).
- La autoridad de control puede exigir al responsable de tratamiento que lleve a cabo esta comunicación cuando no lo haya hecho.

PARA SABER MÁS:

ARTICLE 29 DATA PROTECTION WORKING PARTY 17/EN, WP 250

Guidelines on Personal data breach notification under Regulation 2016/679

Adopted on 3 October 2017

5. ANÁLISIS DE RIESGOS

El enfoque predominantemente «proactivo» del Sistema de Gestión de Datos Personales que se deriva del RGPD impone al responsable y encargado del tratamiento la exigencia de **llevar a cabo con carácter previo un Análisis de Riesgos,** al menos para descartar que deba de realizar una «Evaluación de Impacto relativa a la protección de datos» que se analiza en el siguiente epígrafe de esta Guía.

Esta cuestión está asimismo entrelazada con el Sistema de Seguridad que se implante, pues **el análisis de riesgos debe formar parte de la propia evaluación del nivel de seguridad.**

Y ello lo pone de relieve **el artículo 32.2 RGPD** de forma diáfana:

> *«Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de protección de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos».*

El análisis de riesgos está por tanto imbricado con la seguridad y también con la prevención o anticipación, forma parte «existencial» por tanto del nuevo Sistema de Gestión de Datos Personales, también en el sector público.

Pero ahora nos interesa el Análisis de Riesgo como fase previa a la Evaluación. Y para ello cabe remitirse a un documento que elaboró en su día la AEPD sobre esta cuestión.

PARA SABER MÁS Y COMPRENDER MEJOR QUÉ ES UN ANÁLISIS DE RIESGOS:

Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD (GARTDP, en lo sucesivo)

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

El modelo del RGPD basado en un enfoque de riesgos se despliega con un carácter preventivo con una finalidad muy precisa: garantizar los derechos y libertades de los interesados desde la definición de una actividad de tratamiento.

ISBN: 978-84-7777-543-3

PROTECCIÓN DE DATOS POR DISEÑO Y POR DEFECTO:

El artículo 25 RGPD, tal como se ha dicho, prevé una importante regulación de lo que se enuncia como «Protección de datos desde el diseño y por defecto». Esta regulación es capital para comprender la orientación última del RGPD en un marco de revolución tecnológica acelerada que toma como base sustantiva el dato. Y esa regulación tiene dos dimensiones que siempre se deben cumplir para evitar riesgos:

— *Privacy by design. Garantizar la protección de la privacidad desde el inicio o diseño* (los datos deben protegerse cuando se diseñe un proceso nuevo): Artículo 25.1 RGPD («(…) el responsable del tratamiento aplicará tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas (…) para aplicar de forma efectiva los principios de protección de datos».
— *Privacy by default. Garantizar la protección de la privacidad en todo momento o por defecto.* (los datos deben estar siempre protegidos por defecto). Artículo 25.2 RGPD: «El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento».

LÍNEAS FUERZA DE LA GARTDP (AEPD) SOBRE ANÁLISIS DE RIESGOS:

— FINALIDAD: El diseño adecuado de las actividades de tratamiento es un aspecto clave para poder garantizar los derechos y libertades de los interesados.
— CUÁNDO: La fase de diseño de un tratamiento define el flujo de los datos personales y es el momento idóneo para definir las medidas de control y seguridad para garantizar los derechos y libertades.

—QUÉ ES LA GESTIÓN DE RIESGOS: «Es el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como las medidas para su reducción o mitigación».

—CUÁLES SON LAS ETAPAS DE LA GESTIÓN DE RIESGOS: Es un sistema de monitorización continua que se pueden dividir en tres etapas:

- IDENTIFICAR las amenazas
- EVALUAR los riesgos
- TRATAR los riesgos

—QUÉ ES UNA AMENAZA: «Es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento».

—QUÉ ES UN RIESGO: «Un riesgo se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas».

—TRATAR LOS RIESGOS: «El objetivo de tratar los riesgos es disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen.

—DEFINICIÓN DE LA ACTIVIDAD: Es el paso que requiere tener claros cuáles son las finalidades del tratamiento, así como definir adecuadamente las actividades de tratamiento, documentando los análisis y dejando constancia de la trazabilidad de estos. Se deben tener siempre presentes en este tipo de operaciones los principios del artículo 5 RGPD.

ISBN: 978-84-7777-543-3

IDEA-FUERZA:

El RGPD busca aprovechar las ventajas que ofrece la gestión de riesgos introduciendo una nueva visión donde ***el foco de atención no se centra en las amenazas a la seguridad de la organización, sino que centra su atención en las amenazas sobre los derechos y libertades de los interesados*** (esto es, ciudadanos, clientes, usuarios servicios, etc.). Por tanto, la evaluación de los riesgos debe ser el resultado de una reflexión sobre las implicaciones que los tratamientos de datos de carácter personal tienen en relación con los «interesados»

PARA SABER MÁS Y PARA APLICAR MEJOR LA GESTIÓN DE ANÁLISIS DE RIESGOS:

Es de imprescindible consulta la citada *Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD* elaborada por la AEPD

6. EVALUACIÓN DE IMPACTO SOBRE LA PROTECCIÓN DE DATOS

Conviene tener claro desde el inicio que una Evaluación de Impacto sobre la Protección de Datos (EIPD) no se requiere siempre.

Por eso es importante llevar a cabo con carácter previo el Análisis de Riesgos (aunque en algunos casos, como se verá, no es necesaria esta fase si la EIPD es obligatoria).

El Análisis de Riesgos puede conducir perfectamente a que no existe riesgo alguno en el tratamiento o los riesgos que conlleva son de orden menor (fácilmente controlables), adoptando las medidas técnicas y organizativas necesarias para preservar la seguridad de los datos personales y su no afectación a los derechos y libertades de las personas físicas. En ese caso no hay que pasar a la EIPD.

RECOMENDACIÓN: La *Guía de Análisis de Riesgos en los tratamientos de datos personales sujetos al RGPD* de la AEPD

Indica que «si como resultado del análisis previo se considera que no es necesario llevar a cabo una EIPD, ***se deben documentar adecuadamente los motivos por los cuales se ha llegado a esa conclusión****»,* dejando constancia de que «se ha llevado a cabo ese análisis (responsabilidad proactiva)»

CARÁCTER DE LAS EIPD:

«Las EIPD están orientadas a asegurar preventivamente que, cuando las operaciones de tratamiento puedan comportar riesgos espacialmente relevantes (alto riesgo), se tomen las medidas para reducir, dentro de lo posible, el riesgo de dañar o perjudicar a las personas, o afectar negativamente sus derechos y libertades, impidiendo o limitando su ejercicio o contenido»

Guía Práctica sobre la Evaluación de Impacto relativa a la Protección de Datos 2.0 (GPEI, en lo sucesivo, Barcelona, enero, 2018).

http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/Guia-sobre-la-evaluacion-de-impacto-relativa-a-la-proteccion-de-datos-en-el-RGPD/

EIPD en tratamientos de alto riesgo

CONSIDERANDO 84 RGPD:

«A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento».

ISBN: 978-84-7777-543-3

¿Cuándo llevar a cabo una EIPD?

> CONSIDERANDO 89 «in fine» RGPD
>
> Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial.

El Considerando 90, por su parte, detalla qué son «operaciones a gran escala» y en qué otras operaciones (a raíz, por ejemplo, del tratamiento de «datos de categorías especiales») se requiere EIPD.

Regulación de la eipd en el RGPD

El marco regulatorio de la EIPD está recogido en el importante artículo 35 RGPD. Y en el artículo 36 RGPD se recoge el trámite de «consulta previa» estrechamente relacionado con los tratamientos de alto riesgo.

El artículo 35.1 RGPD establece una regla general que conviene tener siempre presente:

«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. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares».

Por su parte, el artículo 35.3 determina en qué casos la EIPD es necesaria en todo caso en los tratamientos:

a) «Evaluación sistemática y exhaustiva de aspectos personales en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar». En este sentido cabría preguntarse hasta qué punto es posible aprovechar las ventajas que proporciona la Administración electrónica, ser proactivos y utilizar el intercambio de datos personales entre administraciones

públicas para ofrecer, por «anticipación», determinados servicios o prestaciones a la ciudadanía. Una vez más, en estos casos, hay que tener en cuenta todo lo dicho anteriormente.

b) «Tratamiento a gran escala de categorías especiales de datos»
c) «Observación sistemática a gran escala de una zona de acceso público»

La EIPD debe incluir, como mínimo, las exigencias recogidas en el artículo 35.7 del RGPD (Ver más adelante)

Otras cuestiones:

— Para llevar a cabo la EIPD el responsable contará siempre con el asesoramiento de la figura del Delegado de Datos Personales (artículo 35.2).
— Hay que tener en cuenta en esta materia las facultades de las autoridades de control (artículo 35, apartados 4, 5 y 6)
— El cumplimiento de códigos de conducta se tendrán debidamente en cuenta al evaluar las repercusiones de las operaciones realizadas por los responsables o encargados (artículo 35.8 RGPD).

RÉGIMEN DE LA CONSULTA PREVIA: Regulación Artículo 36 RGPD.

— Ante quién se formula: Autoridad de control.
— En qué casos: Cuando la EIPD muestre que el tratamiento entraña alto riesgo
— Papel de la autoridad de control: artículo 36, apartados 2 y 3. Ver asimismo apartado 4.

ALGUNAS ADVERTENCIAS PRELIMINARES SEGÚN LA AEPD SOBRE TRATAMIENTOS ANTERIORES A LA ENTRADA EN VIGOR DEL RGPD:

Guía Práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD (GEIPD)

1. «El RGPD prevé que las Evaluaciones de Impacto se lleven a cabo «antes del tratamiento» en los casos en que sea probable que exista un alto riesgo para los derechos y libertades de los afectados. Ello implica que el mandato del Reglamento no se extiende a las operaciones de tratamiento que ya estén en curso en el momento en que comience a ser de aplicación.

ISBN: 978-84-7777-543-3

2. Sin embargo, sí debiera realizarse una Evaluación cuando en una operación iniciada con anterioridad a la aplicación del Reglamento se hayan producido cambios en los riesgos que el tratamiento implica en relación con el momento en que el tratamiento se pudo en marcha.

3. Este cambio en los riesgos puede derivar, por ejemplo, del hecho de que se hayan empezado a aplicar nuevas tecnologías a ese tratamiento, de que los datos se estén usando para finalidades distintas o adicionales a las que se decidieron en su momento, o de que se estén recogiendo datos distintos o diferentes,

ALGUNAS LÍNEAS FUERZA CONTENIDAS EN LA GEIPD (AEPD) Y EN LA GPEI (apdCAT):

— ALERTA PERMANENTE: «El continuo avance de la tecnología y la evolución de los tratamientos propician la aparición continua de nuevos riesgo que deben ser gestionados: el RGPD exige que los responsable del tratamiento implementen medidas de control»
— EIPD: «La EIPD es una herramienta de carácter preventivo». Se debe reducir el nivel de riesgo a través de determinadas medidas de control «hasta un nivel considerado aceptable».
— ¿CUÁNDO SE DEBE HACER UNA EIPD?: Supuestos de «riesgos elevados». La EIPD está muy vinculada a dos conceptos: «alto riesgo» y tratamiento «a gran escala»
— PRIVACIDAD: La EIPD está alineada con el principio de privacidad y debe cumplir además con los principios de necesidad y proporcionalidad.
— QUÉ DEBE INCLUIR UNA EIPD:

- Una *descripción sistemática de las actividades* de tratamiento previstas
- Una *evaluación de la necesidad y proporcionalidad* del tratamiento respecto a su necesidad
- Una *evaluación de los riesgos*
- Las *medidas para afrontar esos riesgos* (garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales).

- Fases:
  - —Describir el ciclo de vida de los datos
  - —Analizar la necesidad y proporcionalidad de los datos
  - —Gestión de riesgos: Identificar amenazas y riesgos; Evaluar riesgos; y tratar riesgos.
  - —Plan de acción y Conclusiones. Si procede, consulta previa.

— CÓMO DEBE ENTENDERSE LA EIPD: Debe entenderse como un *proceso de mejora continua,* «de forma que esta se revise siempre que se modifique o actualice cualquier aspecto relevante de las actividades de tratamiento».

— QUIÉN DEBE REALIZAR LA EIPD: El responsable del tratamiento. Pero:

- No obstante, «es importante destacar que la responsabilidad del "Responsable" no implica que el área indicada para cada fase de la EIPD sea obligatoriamente quien deba ejecutar las tareas asociadas, pudiendo apoyarse en otras áreas, expertos, recursos externos, etc.».
- La obligación del hacer una EIPD corresponde al responsable del tratamiento, con el apoyo y la colaboración del encargado del tratamiento y con el DPD.
- «Adicionalmente, el personal encargado de la seguridad, el área de tecnología, asesoría jurídica o incluso diferentes responsables de distintas áreas implicadas en el tratamiento pueden ser requeridas durante el proceso de evaluación».

RECOMENDACIÓN GPEI (apdCAT):

«La documentación relacionada con las evaluaciones de impacto debe estar a disposición de las autoridades de supervisión, es decir, no solo el informe final, sino también el conjunto de trabajos que se han utilizado para hacer la evaluación y que sustentan las decisiones tomadas» (p. 15)

— ¿CUÁL ES EL PAPEL DEL DELEGADO DE PROTECCIÓN DE DATOS EN LA EIPD? El papel del Delegado de Protección de Datos en la EIPD es muy relevante. A saber:

ISBN: 978-84-7777-543-3

- Proporciona asesoramiento necesario al responsable del tratamiento para el adecuado desarrollo de la ejecución de la EIDP.
- «Supone un valor añadido en el desarrollo de la EIPD aportando garantías para los derechos y libertades de los interesados».
- «Puede haber sido el mismo delegado de protección de datos quién haya definido cómo se debe ejecutar las EIPD en la organización (por ejemplo, mediante la elaboración de una guía interna de evaluación o adoptando una guía externa que sirva de marco de evaluación); y asimismo, quien ejecute la evaluación» (GPEI)
- El DPD debe verificar la adecuada ejecución de la EIPD

—METODOLOGÍA (Ver GEIPD, pp. 10-36):

- Contexto del tratamiento: Conocer ciclo de vida y flujo de los datos
- Gestión de Riesgos:
  - —Identificar
  - —Evaluar
  - —Tratar
- Comunicación y Consulta a la autoridad de control
- Supervisión y revisión de la implantación: papel del DPD.

ORIENTACIONES PARA LA EJECUCIÓN DE LA EIPD SEGÚN LA GPEI (ACPD):

—**Aspectos preparatorios de la ejecución de la EIPD:** Método de evaluación, interlocutores, equipo de evaluación, etc.

—**Análisis de la necesidad de hacer la EIPD:** ¿Qué datos se tratarán y de quién? (elaborar lista exhaustiva); Volumen de personas afectadas por el tratamiento y si este es «a gran escala»; ¿Qué se prevé hacer con los datos?

—**Descripción sistemática de las operaciones de tratamiento** (descripción funcional según el ciclo de los datos)

— **Objetivos y finalidades del tratamiento:** evaluación necesidad y proporcionalidad de las operaciones de tratamiento.
— **Gestión de Riesgos:** aspectos generales. Identificación de potenciales escenarios de riesgo (PER)
— **Informe de Evaluación:** Conclusiones y Recomendaciones para mitigar los riesgos de las operaciones de tratamiento.

IDEA FUERZA:

La gestión de riesgos que prevé el RGPD va más allá de evaluar la exposición al riesgo de los sistemas de información o de los datos o de los riesgos para la organización (GPEI/apdCAT, p. 61).

IDENTIFICACIÓN DE SITUACIONES DE RIESGO SEGÚN RGPD GPEI/apdCAT (p. 61):

— Se priva a los interesados de sus derechos y libertades, que incluye cuando se impide su ejercicio normal y libre.
— Se provocan daños y perjuicios físicos, materiales o inmateriales a las personas interesadas.
— Se revelan categorías especiales de datos personales, o relativas a condenas e infracciones penales, durante el tratamiento.
— Se crean o se utilizan perfiles personales.
— Se tratan los datos personales de colectivos especialmente vulnerables
— Se trata una gran cantidad de datos personales o datos que afectan a un gran número de personas

ISBN: 978-84-7777-543-3

CUATRO CUESTIONES CLAVE EN UNA EIPD (GEIPD, AEPD):

1. En ningún caso se puede proceder a llevar a cabo un tratamiento sl el riesgo es elevado.
2. En aquellos casos en que se presta un servicio como encargado de tratamiento se recomienda realizar un análisis de riesgos sobre la tipología del servicio prestado.
3. Siempre que exista una variación relevante en el contexto de las actividades de tratamiento que pueda suponer un incremento del riesgo asociado al mismo, deberá realizarse una actualización de la EIPD.
4. Si el responsable del tratamiento está adherido a algún código de conducta donde se incluya metodología propia, se podrá utilizar la misma para la realización de las EIPD.

PARA SABER MÁS:

GT29 WP 248; *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento entraña probablemente un alto riesgo a efectos del Reglamento (UE) 2016/279*

http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/altres_documents_del_grup_de_larticle_29/

IDEA-FUERZA FINAL:

Una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento (GPEI/adpCAT, p. 7)

SMART CITIES: UN EJEMPLO DE EIDP SEGÚN LA AEPD

— « Antes de la puesta en producción de un proyecto *Smart City* es necesario hacer un análisis previo del mismo valorando el volumen de la información que se pretende procesar y el número y tipo de fuentes desde la que se pretende obtener dicha información o incluso el tiempo durante el que se pretende conservar esta información»
— Por tanto, en estos casos, «será necesaria la realización de una evaluación de impacto relativa a la protección de datos o incluso una consulta previa a la autoridad de protección de datos» (p. 24)

AEPD, *Protección de datos y Administración Local*

7. EL DELEGADO DE PROTECCIÓN DE DATOS

La figura del Delegado de Protección de Datos (DPD) es nueva, aunque tiene algunos precedentes que ahora no es necesario citar.

Se inserta, como una pieza más e importante, en el nuevo Sistema Institucional y de Gestión de Datos Personales que se enmarca en esa política «proactiva», anticipatoria o preventiva por la que aboga el RGPD.

Para las Administraciones Públicas la nota más importante es la obligatoriedad que establece el RGPD: todas ellas deben disponer de un DPD.

Realmente, esa exigencia, como tantas otras que se contienen en el RGPD, iban más dirigidas a las Administraciones Públicas de gran tamaño y a otras sectoriales donde los riesgos, el uso masivo y las categorías especiales en el tratamiento de datos personales son la moneda corriente. Pero la obligación normativa está ahí y, por tanto, ha de cumplirse, también por todas las Administraciones Locales.

Hay que insertar la figura del DPD en ese cambio de modelo de gestión de datos personales al que se viene haciendo referencia. Y hay que verlo como ventana de oportunidad, pues el DPD debería ayudar a ese proceso de transformación organizativa y al cambio en los tratamientos que el RGPD exige.

ISBN: 978-84-7777-543-3

Esa transformación o tránsito de una cultura «reactiva» a otra «proactiva» no es fácil, menos aún en un sector público en el que el endurecimiento del régimen sancionador del RGPD se ve hasta cierto punto descafeinado, al descansar principalmente sobre «multas administrativas», que de momento no parece que se vayan a proyectar sobre los responsables o encargados del tratamiento en las Administraciones Públicas (según redacción del artículo 77.1 PLOPD).

En ese contexto, el DPD debe ser una palanca de transformación que haga posible la implantación de la cultura proactiva también en las instituciones públicas y, por lo que ahora interesa, en la Administración Local.

Pero, además, el DPD es importante que tenga conocimientos especializados y cualificación pertinente, pues es el punto de apoyo principal del responsable y encargado del tratamiento (esto es, quien les asesora), al efecto de cumplir debidamente las obligaciones del RGPD. Debería actuar, por tanto, como «cortafuegos» que impidiera incumplimientos. Especialmente importante es su papel en los procesos de Evaluación de Impacto.

Es en el considerando 97 dónde se dibujan las líneas maestras de esa nueva figura del DPD, que luego serán desarrolladas por los artículos 37 a 39 del RGPD, así como a través de referencias incidentales (algunas que ya se han visto) a lo largo del resto del articulado.

CONSIDERANDO 97 RGPD:

«Al supervisar la observancia interna del presente Reglamento, ***el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública,*** *a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial (…)* ***Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente.»***

Cuatro son, por tanto, las ideas-fuerza que cabe resaltar del DPD según este Considerando 97:

1. El DPD es un colaborador necesario, aunque también supervisor, del responsable o encargado del tratamiento en el sector público.
2. Debe ser DPD una persona que acredite conocimientos especializados del Derecho y de la práctica de protección de datos.
3. El DPD puede ser empleado público o ser provisto de forma externa.
4. El DPD ejerce sus funciones y cometidos «de manera independiente»

Antes de adentrarnos en el análisis de la regulación normativa y en algunos aspectos operativos o prácticos que plantea a corto plazo esta figura, es conveniente delimitar su alcance en el ámbito de lo que hasta ahora indeterminadamente llamamos «sector público»

¿Qué cabe entender por «autoridad y organismo público» según el RGPD?

El RGPD utiliza *la expresión «autoridad y organismo público»* a la hora de atribuir la exigencia de crear necesariamente la figura del DPD.

¿Y qué cabe entender por «autoridad y organismo público» según el RGPD?

Esta es una noción que, como expuso el Grupo de Trabajo del Artículo 29 en el documento que seguidamente se cita (*Directrices sobre los delegados de protección de datos*), reenvía al Derecho interno de los Estados miembros.

Y, por tanto, tendría que ser la futura LOPD la que precisara su perímetro. De momento, la redacción que se ha dado al artículo 34 PLOPD es sencillamente frustrante, pues seguimos sin saber con certeza qué entidades del sector público son las que están obligadas a disponer de esta figura del DPD.

Para resolver el problema (al menos hasta que la LOPD se apruebe definitivamente) se puede intentar acudir al artículo 77 PLOPD, donde se regula cuál es el «Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento» que, por una razón de paralelismo, cabría estimar que son las entidades que sí tienen obligación de disponer de un DPD. Por lo que afecta al ámbito local de gobierno, el perímetro de aplicación de tal régimen singular se proyecta sobre las siguientes entidades:

— Los entes que integran la Administración Local (Ayuntamientos, Veguerías o Diputaciones, Áreas Metropolitanas, Comarcas, Mancomunidades y Entidades Municipales Descentralizadas)

ISBN: 978-84-7777-543-3

— Los organismos públicos y entidades de Derecho Público vinculadas o dependientes de la Administración Local (organismos autónomos y entidades públicas empresariales)
— Las fundaciones del sector público adscritas a entes locales.
— Los consorcios adscritos a un ente local.

Si se puede trasladar ese esquema institucional a las entidades que están obligadas a disponer de un DPD, ello supondría que las sociedades mercantiles no tendrían esa obligación «ex RGPD», pero que sí podría exigírseles en los mismo términos que a las empresas del sector privado cuando concurrieran las circunstancias previstas en el citado RGPD.

Pero no parece tener mucho sentido que se incluya a las Fundaciones y no a las sociedades mercantiles de capital público. Algunas de ellas llevan a cabo precisamente tratamiento de datos de forma extensa e intensa (piénsese, por ejemplo, en todas aquellas sociedades mercantiles de capital público muy presentes en la escena vasca que prestan servicios informáticos de apoyo a la entidad matriz). Por tanto, lo más recomendable es que, dado que también en aquellos supuestos en los que las entidades o empresas no tengan la obligación de dotarse de un DPD lo puedan hacer, las sociedades mercantiles designen también un DPD o, en su caso, de acuerdo con lo establecido en el artículo 37.2 RGPD, se valgan de aquel que haya sido designado por la Administración Pública a la que estén vinculadas.

PARA SABER MÁS:

Directrices sobre los delegados de protección de datos (DPD), adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017, Grupo de Trabajo sobre la protección de Datos del Artículo 29. 16/ES WP 243, rev. 1

http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/altres_documents_del_grup_de_larticle_29/

La regulación de esta figura se recoge principalmente en los artículos 37 a 39 RGPD.

El artículo 37, dedicado a **«la designación»** del DPD, prevé los siguientes extremos:

— DESIGNACIÓN PRECEPTIVA: ¿Cuándo ha de designarse según el RGPD por el responsable del tratamiento preceptivamente un DPD? (artículo 37.1 RGPD) El caso de las autoridades y organismos públicos ya ha sido analizado. Lo que no impide que cualquier organización lo pueda designar voluntariamente o si así lo exige la legislación de un Estado miembro (artículo 37.4 RGPD)
— ¿CUÁNTOS DPD?: Pretende dar respuesta a si cabe nombrar uno o varios DPD (por grupo de empresas o autoridad u organismo público, atendiendo a «su estructura organizativa y su tamaño» (artículo 37.2 y 3 RGPD)
— ACREDITACIÓN COMPETENCIAS PROFESIONALES: Las exigencias profesionales y conocimientos que debe acreditar quien sea designado DPD, vinculadas a las funciones de la figura (artículo 37.5 en relación con artículo 39 RGPD)
— ¿INTERNO O EXTERNO? El DPD podrá formar parte de la plantilla o ser un externo a la organización (contratación de servicios) (artículo 37.6 RGPD)
— PUBLICIDAD DEL DPD: El responsable o encargado publicarán (presumiblemente en la Web o Portal de Transparencia) los datos de contacto del DPD y los comunicarán a la AVPD.

Por su parte, el artículo 38 tiene como objeto **«la posición»** del DPD en relación con el responsable o encargado del tratamiento:

— COLABORADOR NECESARIO: Se prevé una garantía de participación del DPD en «todas las cuestiones relativas a la protección de datos personales» (artículo 38.1 RGPD).
— RECURSOS: Se le deben facilitar al DPD los recursos necesarios para el desempeño de sus funciones y para el mantenimiento de sus conocimientos especializados (formación) (artículo 38.2 RGPD)
— ESTATUTO INDEPENDENCIA: Garantía de que no recibirá ninguna instrucción en lo que respecta al desempeño de sus funciones, no pudiendo ser destituido ni sancionado por su desempeño, y rindiendo cuentas al más alto nivel jerárquico de la organización (artículo 38.3 RGPD)
— PUNTO DE CONTACTO: Los interesados podrán ponerse en contacto con el DPD en todo lo relativo a sus datos personales y al ejercicio de sus derechos (artículo 38.4 RGPD).
— CONFIDENCIALIDAD: El DPD está obligado a mantener el secreto o confidencialidad por el desempeño de sus funciones (artículo 38.5 RGPD)

ISBN: 978-84-7777-543-3

— DPD «A TIEMPO PARCIAL»: El DPD podrá desempeñar otras funciones siempre que no den lugar a conflictos de interés (artículo 38.6 RGPD)

Y, en fin, el artículo 39 RGPD define cuáles son, como mínimo, las funciones del DPD, vinculándolas todas ellas especialmente a «los riesgos asociados a las operaciones de tratamiento»(artículo 39.2 RGPD). A saber:

FUNCIONES DEL DPD SEGÚN EL RGPD:

— Informar y asesorar al responsable o al encargado del tratamiento y a los empleados sobre las obligaciones del RGPD y del Derecho interno.
— Supervisar el cumplimiento del presente RGPD, promover su implantación en la organización e impulsar la formación.
— Ofrecer asesoramiento sobre la EIPD y supervisar su aplicación.
— Cooperar con la autoridad de control.
— Actuar como punto de contacto de la autoridad de control.

Por su parte, ha de ser la futura LOPD la que complete algunos de los perfiles de ese régimen jurídico de la figura del DPD definida por el RGPD.

El PLOPD contiene, por ejemplo, las siguientes previsiones (artículos 34 a 37):

— Obligación de comunicar a la AVPD en el plazo de 10 días las designaciones, nombramientos y ceses de los DPD
— La AVPD mantendrá una lista actualizada de DPD que será accesible por medios electrónicos.
— Por Real Decreto se establecerá el procedimiento de interconexión de las listas creadas por las autoridades de control (AEPD/AVPD/apdCAT).
— La acreditación de los «requisitos» exigidos por el RGPD podrá realizarse, entre otros medios, a través de mecanismos voluntarios de certificación
— La remoción del DPD se podrá realizar si incurriera en dolo o negligencia grave en el ejercicio de sus funciones, previo expediente disciplinario tramitado al efecto (sector público).
— El DPD tendrá acceso a todos los datos personales y procesos de tratamiento.

— Cualquier vulneración relevante en materia de protección de datos será comunicada por el DPD al responsable o encargado del tratamiento.
— Con carácter previo a la interposición de una reclamación antes la autoridad de control por parte del interesado, este «podrá dirigirse al DPD de la entidad contra la que se reclame». En este caso, el DPD «comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación».
— Si el afectado presenta la reclamación ante la AVPD, esta podrá remitir la reclamación al DPD a fin de que responda en el plazo de un mes. En caso de no respuesta, continuará el procedimiento.

ALGUNAS DIRECTRICES DE LAS AUTORIDADES DE CONTROL SOBRE LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS:

El Delegado de Protección de Datos en las Administraciones Públicas

http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php

PARA SABER MÁS:

Rafael Jiménez Asensio, «La figura del Delegado de Protección de Datos en las organizaciones públicas», *La Mirada Institucional*

https://rafaeljimenezasensio.com/2018/03/20/la-figura-del-delegado-de-proteccion-de-datos-en-las-organizaciones-publicas-1/

Víctor Almonacid, «El Delegado de Protección de Datos en la Administración Local»

https://nosoloaytos.wordpress.com/2018/03/28/el-delegado-de-proteccion-de-datos-en-la-administracion-local-dpo/#more-13764

Concepción Campos Acuña, «Los 7 imprescindibles en protección de datos para el ámbito local», *El Consultor de los Ayuntamientos y Juzgados,* enero 2018

ISBN: 978-84-7777-543-3

IDEAS-FUERZA Y PROBLEMAS APLICATIVOS DE LA IMPLANTACIÓN DE LA FIGURA DEL DPD EN LAS ADMINISTRACIONES LOCALES

¿CUÁNTOS DPD DEBE HABER EN LAS AAPP?:

— Uno al menos, en las Administraciones Públicas de cierto tamaño pueden ser dos o más, según sectores. Nada impide, sin embargo, que sea un solo DPD con una unidad o departamento y actuando de forma descentralizada.

¿LOS GOBIERNOS LOCALES DE PEQUEÑO O MEDIANO TAMAÑO DEBEN TENER DPD?

— Necesariamente, pero esa función se puede prestar por las Diputaciones forales, entidades supramunicipales o, en su caso, a través de Mancomunidades o por medio de Convenios entre entes locales (horizontales o verticales).

¿PUEDEN SER DPD ÓRGANOS COLEGIADOS?

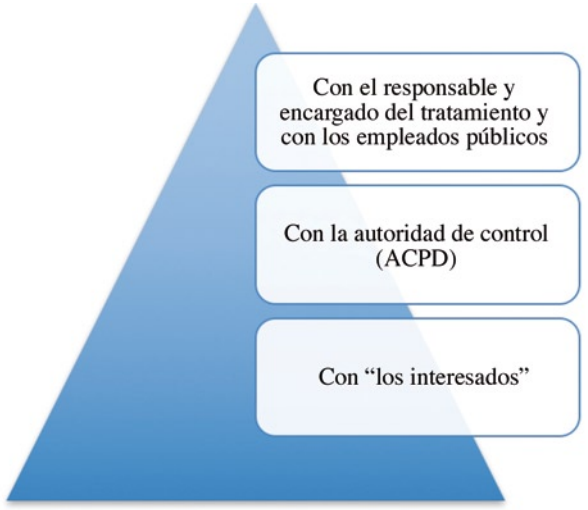
— El GT-ART-29 lo desaconseja; la accesibilidad requiere personalización.

¿DEBE SER EL DPD FUNCIONARIO O EMPLEADO PÚBLICO?

— Preferentemente sí, siempre que realice funciones de autoridad (funcionario), pero cabe la externalización de los servicios, aunque no de aquellas funciones que directa o indirectamente ejerzan potestades públicas. Las funciones del RGPD pueden ejercerse por un externo (empresa o profesional), las que asigna el PLOPD pueden plantear más dudas.

¿CABE QUE EL DPD DESARROLLE SUS FUNCIONES A TIEMPO PARCIAL? Sí, siempre que no se vea incurso en conflictos de interés.

POSICIÓN DEL DPD Y FUNCIONES: LA RELACIÓN TRIANGULAR DEL DPD



FUNCIONES DEL DPD:

—RGPD fija funciones mínimas. Derivan de su relación «triangular»
—Atención especial a los riesgos en las operaciones de tratamiento
—Las funciones esenciales son:

- Asesorar responsable y encargado de tratamiento
- Asesorar, orientar sobre análisis de riesgo y ejecutar, incluso, los EIPD
- Supervisar cumplimiento RGPD
- Cooperar con la autoridad de control
- Actuar como punto de contacto
- Conocer de las reclamaciones previas Protección de Datos y por remisión de la autoridad de control (PLOPD)

ISBN: 978-84-7777-543-3

CUALIDADES PROFESIONALES QUE DEBE ACREDITAR EL DPD:

—Cualidades profesionales y conocimientos especializados:

- Conocimientos y experiencia de Derecho Público (*Directrices*: procedimientos administrativos)
- Conocimientos y experiencia de Protección de Datos
- Buen manejo del RGPD y de todos los instrumentos allí recogidos

—Qué ámbito profesional es el más idóneo para el desarrollo de esas funciones

- No hay reserva de tales funciones a una profesión determinada. Pero el PLOPD le da un sesgo jurídico acusado: resolver reclamaciones (aunque eso puede subsanarse con personal técnico adscrito)
- Las *Directrices* añaden también integridad y ética (inciden mucho en cómo evitar conflictos de intereses).

ESTATUTO JURIDICO Y POSICIÓN DEL DPD:

—Independencia: no recibe instrucción alguna. No tiene dependencia jerárquica.
—Participación temprana en los procesos de tratamiento de datos.
—Presencia en los órganos que adaptan decisiones (problema con externos)
—Proveer de los recursos necesarios si es interno (local, medios personales y tecnológicos)
—Facilitarle formación para el mantenimiento de sus conocimientos
—«Tiempo suficiente» para el ejercicio de sus funciones
—A mayor complejidad del tratamiento más recursos
—Rendición de cuentas al máximo nivel (externos)
—Blindaje frente a sanciones (PLOPD) y remociones
—Mantener secreto y confidencialidad

UBICACIÓN ORGÁNICA DEL DPD:

- ¿Cómo encuadrarlo en la estructura?
- Descartar su encuadre como alto cargo.
- Unidad situada en presidencia o vinculada a órganos superiores, en el ámbito local en alcaldía o en la presidencia. Motivos.
- Cubierta preferentemente por funcionario A1. No necesariamente jurista.
- Figura incardinada en el modelo de Seguridad informática.

ALGUNOS PROBLEMAS DE RRHH EN RELACIÓN AL DPD: LISTADO DE CUESTIONES ABIERTAS

- Crear un puesto de trabajo *ad hoc* o acumular las funciones a otro existente.
- Incorporar a plantilla presupuestaria y a la RPT, en su caso
- ¿Cómo cubrir ese puesto de trabajo?
  - Selección «ex novo» desaconsejable. Razones,
  - Cubrirlo con funcionarios interinos, desaconsejable también.
  - ¿Se puede designar personal laboral? Plantea dificultades (PLOPD)
- *La primera tensión: discrecionalidad y profesionalidad*. Debe primar esta última: criterios de competencia profesional.
- Provisión puesto DPD. Modalidades
  - Libre designación. Desaconsejada, no se ajusta RGPD.
  - Concurso de méritos, no mide competencia profesional efectiva
  - Concurso específico, puede ser el más idóneo
  - ¿Cabe la comisión de servicios y otras formas de provisión?

ISBN: 978-84-7777-543-3

— *La segunda tensión: temporalidad versus permanencia*. Decisión estratégica: puesto de estructura permanente, pero cubierto por períodos. No hay (casi) profesionales de ese perfil. Importancia estratégica.

- Decisión compleja en un primer momento, aunque RGPD parece dar carácter estructural a la figura, ello no impediría rotación.
- Dificultades, marco jurídico rígido.
- Se podría explorar la figura de la DPP como alternativa. Problemas: normativización.

ÁRBOL DE DECISIONES EN RELACIÓN CON EL DPD EN LAS ADMINISTRACIONES PÚBLICAS:

1. Internalizar o externalizar la figura. Valorar «pros» y «contras». Prestar servicios por otra Administración (definición del convenio). Prestar servicios externos (definición pliegos de contratación).
2. Uno o varios DPD.
3. Cómo y dónde encuadrarla en la estructura organizativa. No dependencia.
4. Dotarla de medios: ¿estructura personal?
5. A tiempo completo o parcial
6. ¿Qué régimen jurídico aplicamos?
7. ¿Qué sistema de provisión?
8. ¿Cómo salvaguardar su independencia?

ALGUNAS CONCLUSIONES:

— Figura singular y de complejo encaje. Prueba ensayo/error
— Irá creciendo en protagonismo conforme avance la revolución tecnológica
— Banco de pruebas para explorar la incorporación de nuevos perfiles
— La exigencia de inscripción se difiere a la aprobación de la LOPD. Se gana tiempo.
— *Factor tiempo:* Nos hemos despertado muy tarde y sin las herramientas necesarias

8. CÓDIGOS DE CONDUCTA Y MECANISMOS DE CERTIFICACIÓN

Se trata de **dos instrumentos que entroncan perfectamente con el enfoque «proactivo» que imprime el RGPD**. Tienen, por tanto, una orientación preventiva o anticipatoria.

Asimismo **son herramientas de carácter voluntario, pero** que en el caso de los Códigos de Conducta, **una vez asumidos por quienes se adhieran a los mismos tendrán carácter vinculante.**

En cualquier caso, sin perjuicio de lo que se dirá, cabe presumir que la adhesión a tales códigos puede implicar la atenuación en sus caso de las responsabilidades derivadas por un tratamiento de datos incorrecto. Aunque, en el supuesto de los mecanismos de certificación, expresamente se recoge la idea de que la certificación no limitará la responsabilidad del responsable o del encargado (artículo 43.4 RGPD). De ahí que se hablara al inicio de este trabajo de una *política de compliance* atenuada trasladada a la protección de datos.

Códigos, certificación y política de cumplimiento

Esa impresión inicial puede desvanecerse si se analizan estas herramientas en el marco del conjunto de previsiones del RGPD.

En efecto, los rasgos del sistema preventivo y de cumplimiento son evidentes en ciertos pasajes del RGPD. Tal como prevén los artículos 24.3 y 28.5 RGPD, **la adhesión a códigos de conducta o mecanismos de certificación «pueden ser utilizados como elementos para demostrar el cumplimiento»** o la existencia de una serie de garantías, respectivamente, **por parte del responsable o del encargado del tratamiento.**

Asimismo, la adhesión a un Código de Conducta o a un mecanismo de certificación «podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos» (en materia de seguridad) en el artículo 32.1 RGPD (artículo 32.3 RGPD).

También el cumplimiento de los códigos de conducta «se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por los responsables o encargados», en particular cuando se lleve a cabo una EIPD.

ISBN: 978-84-7777-543-3

IDEA-FUERZA:

Por consiguiente, **disponer de códigos de conducta y mecanismos de certificación es** no solo adoptar una visión preventiva en línea con la finalidad del RGPD, *sino especialmente* ***dotarse de una política de cumplimiento que salvaguarda la función del responsable o encargado del tratamien****to de cualquier organización pública (Administración autonómica o foral, así como en su sector público), también de la Administración Local.*

Regulación códigos de conducta

En el RGPD

El RGPD regula en los artículos 40 a 43 los códigos de conducta y los mecanismos de certificación. A pesar de su carácter de libre adhesión, cabe constatar que algunas de tales previsiones no se aplican a «las autoridades y organismos públicos».

El artículo 40.1 RGPD prevé una labor de promoción de los códigos de conducta que será llevada a cabo, por lo que ahora interesa, por la AVPD (o el resto de autoridades de control), en la que se tendrán en cuenta las características específicas de los distintos sectores de tratamiento.

IDEA-FUERZA:

Los códigos de conducta están destinados a contribuir a la correcta aplicación del RGPD (artículo 40.1)

Por su parte, el artículo 40.2 se refiere a que «las asociaciones y otros organismos representativos de categorías de responsables o encargados de tratamiento *podrán* elaborar códigos de conducta». Como podría ser, por ejemplo, el caso de EUDEL o de las demás asociaciones o federaciones de municipios o entes locales, en su caso.

Y se establece un contenido orientativo de lo que pueden recoger tales códigos. Por ejemplo (Ver artículo 42.2 RGPD):

— La recogida de datos personales
— La información proporcionada al público y a los interesados
— El ejercicio de los derechos del interesado
— Las medidas y procedimientos para garantizar la seguridad del tratamiento
— La notificación y comunicación de las violaciones de la seguridad de los datos, respectivamente, a la autoridad de control y a los interesados

Es importante, asimismo, tener en cuenta que tales asociaciones que promuevan esos códigos de conducta (por ejemplo, EUDEL, FEMP, FMC o ACM) deben presentar el **proyecto de código ante la autoridad de control** (AVPD o la autoridad que corresponda: AEPD o apdCAT) **para que por parte de esta se dictamine si es conforme al RGPD y proceda a aprobar tal código** «si considera suficiente las garantías adecuadas ofrecidas». Por parte de la autoridad de control se registrará y publicará tal código (artículo 40.5 y 6 RGPD).

> ACLARACIÓN (Exclusión autoridades y organismos públicos):
>
> Cabe tener en cuenta que el artículo 41 RGPD («Supervisión de los códigos de conducta aprobados»), así como por conexión el artículo 40. 4 RGPD, no se aplicarán al tratamiento realizado por autoridades y organismos públicos (artículo 41.6 RGPD)

En el PLOPD

La regulación (provisional) de los códigos de conducta en el PLOPD se contiene en su artículo 38 y tiene, por lo que a la Administración Local interesa, los siguientes rasgos:

— Los códigos de conducta serán vinculantes por quienes se adhieran a los mismos.
— Podrán promoverse por asociaciones y organismos, pero también por los responsables o encargados a los que se refiere el artículo 77.1 LOPD. Por tanto, por cualquier ente local, organismo público, consorcio o fundación.

ISBN: 978-84-7777-543-3

— Los códigos serán aprobados por las autoridades de control (en este caso por la AVPD)
— Las autoridades de control someterán los proyectos de código de conducta al mecanismo de coherencia establecido en el artículo 63 RGPD, en relación con lo previsto en el artículo 40.7 RGPD.
— La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán un registro conjunto de los códigos de conducta aprobados.
— Por Real Decreto se establecerá el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta.

Regulación mecanismos de certificación

En el RGPD

Los artículos 42 y 43 RGPD regulan los mecanismos y organismos de certificación.

En el artículo 42.1 también se recoge una labor de «promoción» que debe ser ejercida entre otros por los Estados miembros y las autoridades de control con la finalidad de crear mecanismos de certificación en materia de protección de datos y sellos y marcas de protección de datos. El objetivo de tales instrumentos es siempre «demostrar el cumplimiento de lo dispuestos en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados»

IDEA-FUERZA:

Los mecanismos de certificación (sellos o marcas) tienen como finalidad principal demostrar que, por parte de los responsables y encargados del tratamiento, se cumple el RGPD. Tienden, por tanto, a salvaguardar la actuación de responsables y encargados. De ahí la importancia de dotarse de ellos.

Las líneas básicas de esa regulación son las siguientes:

- La certificación será voluntaria y estará disponible a través de un proceso transparente (artículo 42.3 RGPD).
- La certificación no limitará las responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento (artículo 42.4 RGPD)
- Será expedida por los organismos de certificación regulados en el artículo 43 RGPD o por la autoridad de control competente (AVPD), sobre la base de criterios aprobados por dicha autoridad en los términos establecidos en el artículo 42 RGPD.
- Obligación de los responsables y encargados del tratamiento de proveer toda la información necesaria para llevar a cabo el procedimiento de certificación.
- La certificación será expedida al responsable o encargado del tratamiento por un período máximo de tres años, renovables en las condiciones expuestas (artículo 42.6 RGPD)

En el PLOPD

El artículo 39 PLOPD confiere la competencia para llevar a cabo la acreditación de las instituciones de certificación a la Entidad Nacional de Acreditación (ENAC), que será la que comunique a las autoridades de control respectivas (en este caso, AVPD) las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

Se ha de tener asimismo en cuenta la disposición transitoria segunda del PLOPD en relación con los Códigos tipo inscritos en las autoridades de protección de datos de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre: Adaptación de su contenido al artículo 40 RGPD en el plazo de un año.

UNA BUENA PRÁCTICA:

Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD)

http://www.agpd.es/portalwebAGPD/temas/certificacion/index-ides-idphp.php

ISBN: 978-84-7777-543-3

9. AUTORIDADES DE CONTROL INDEPENDIENTES: IDEA GENERAL

No cabe duda que la correcta implantación del RGPD, también en los distintos niveles de gobierno (y, en particular, en la Administración Local) requiere de esa pieza institucional imprescindible que son las autoridades de control.

No es objeto de este trabajo, por sus especiales características, analizar el papel y funciones de tales autoridades de control, a las que el RGPD y el PLOPD dedican un buen espacio regulador.

En estas páginas solo interesa destacar cuál es la finalidad de tales autoridades de control, en especial de la AVPD (aunque también sus relaciones con la AEPD y con la apdCAT), y poner de relieve algunos de sus elementos más relevantes, pues se trata sin duda, del mecanismo de cierre para que el nuevo Sistema Institucional y de Gestión de Protección de Datos de las Administraciones Públicas funcione adecuadamente.

Bajo este punto de vista es oportuno resaltar que **la finalidad principal de las autoridades de control no es otra que la protección de las personas físicas con respecto al tratamiento de datos de carácter personal**.

Esta es una idea que se recoge perfectamente en el Considerando 117 y en otros sucesivos (por ejemplo, en el Considerando 123 donde se añade a la finalidad anterior la de «facilitar la libre circulación de los datos personales en el mercado interior»). En el ejercicio de esas funciones «deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión».

> CONSIDERANDO 117 RGPD
>
> *El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa.*

No interesa abordar aquí las cuestiones relativas a la posición institucional de estas autoridades de control ni tampoco a la existencia de varias autoridades de control o a la designación, en este caso, de una autoridad de control que ejerza como «punto de contacto único» (Considerando 117). Pero sí puede ser oportuno resaltar que los amplios cometidos funcionales que el RGPD encomienda a tales autoridades de control implicarán necesariamente un refuerzo de recursos financieros y humanos, que no parece ser muy viable en época de contención fiscal.

Regulación de las autoridades de control en el RGPD

La regulación de las autoridades de control en el RGPD está contenida en su Capítulo VI. Este Capítulo se estructura en diferentes secciones que abordan, entre otros, los siguientes ámbitos materiales:

- Designación de una o varias autoridades por Estado (actualmente en España existen tres: AEPD, AVPD y apdCAT; pues sigue sin haberse activado aún la ATPD de Andalucía) (artículo 51 RGPD)
- Estatuto de independencia de tales autoridades (ajenos a toda influencia externa, ya sea directa o indirecta y no admitirán ninguna instrucción) (artículo 52 RGPD)
- Condiciones aplicables a los miembros de las autoridades de control y normas relativas al establecimiento de la autoridad de control. (artículos 53 y 54 RGPD)
- Competencias de la autoridad principal de control (artículos 55 y 56 RGPD)
- Funciones es el aspecto más importante a nuestros efectos y se trata de forma singularizada (artículo 57 RGPD)
- Poderes, que se desdoblan en poderes de investigación, correctivos o de autorización y consultivos (artículo 58 RGPD).
- Informe de actividad (artículo 59 RGPD)

ISBN: 978-84-7777-543-3

ALGUNAS FUNCIONES DE LAS AUTORIDADES DE CONTROL EN RELACIÓN CON LOS GOBIERNOS LOCALES:

- —Controlar la aplicación del presente Reglamento y hacerlo aplicar.
- —Asesorar a las instituciones sobre las medidas administrativas a adoptar para la protección de los derechos y libertades con respecto a los tratamiento de datos.
- —Promover la sensibilización de los responsable y encargados del tratamiento sobre sus obligaciones derivadas del presente Reglamento.
- —Tratar las reclamaciones presentadas.
- —Llevar a cabo investigaciones sobre aplicación del presente Reglamento.
- —Adoptar cláusulas contractuales tipo
- —Elaborar lista relativa al requisito de Evaluación de Impacto.
- —Ofrecer asesoramiento sobre operaciones de tratamiento.
- —Alentar la elaboración de códigos de conducta, dictaminar y aprobarlos.
- —Fomentar la creación de mecanismos de certificación de la protección de datos y aprobar los criterios de certificación.
- —(El desempeño de las funciones de la autoridad de control será gratuito para el interesado y para el delegado de protección de datos; salvo las excepciones tasadas en la norma (artículo 57.4 RGPD).

ALGUNOS «PODERES CORRECTIVOS» DE LAS AUTORIDADES DE CONTROL SEGÚN EL RGPD

- Sancionar a todo responsable o encargado del tratamiento con una advertencia.
- Sancionar a todo responsable o encargado del tratamiento con un apercibimiento
- Ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del RGPD
- Ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten al RGPD
- Ordenar al responsable de tratamiento que comunique las violaciones de la seguridad de los datos personales.
- Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.
- Ordenar la rectificación o supresión de datos personales o la limitación de tratamiento.
- Retirar una certificación
- Imponer una multa administrativa (ver régimen singular entidades sector público)

Regulación de las autoridades de control en el PLOPD

El Título VII del PLOPD regula exhaustivamente las Autoridades de protección de datos.

No puede ser objeto de este trabajo un análisis detenido de tales previsiones, máxime el carácter provisional que ellas tienen al encontrarse en plena tramitación parlamentaria el proyecto de Ley.

Por tanto, solo se dará noticia puntual de algunos de los puntos de esa propuesta normativa a efectos de pura información y obviamente de aquellos que puedan afectar con mayor intensidad a las entidades locales.

Algunos aspectos de interés de esa regulación a efectos del presente trabajo serían los siguientes:

- En el Capítulo relativo a la Agencia de Española de Protección de Datos, conviene resaltar lo siguiente:
  - En el ámbito de las potestades de investigación y planes de auditoria preventiva hay que tener en cuenta lo dispuesto en el

ISBN: 978-84-7777-543-3

artículo 51 sobre ámbito de la investigación y personal competente para llevarla a cabo.
- Igualmente es importante el deber de colaboración de las Administraciones Públicas establecido en el artículo 52.
- Las potestades de regulación a través de «Circulares de la Agencia Española de Protección de Datos»
- O las funciones relacionadas con la Acción exterior.

— En el Capítulo relativo a las Autoridades autonómicas de protección de datos, se contienen algunas previsiones importantes en el ámbito autonómico, foral y local. Por ejemplo, dos de ellas vinculadas con el ejercicio que a tales autoridades de control se les reconoce de las funciones establecidas en los artículos 57 y 58 RGPD, cuando se refieran a:

  - Tratamientos de los que sean responsable las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.
  - Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómico o Local. Obviamente, también de las Administraciones forales.

— Cabe presumir igualmente que la normativa reguladora de las Autoridades de control de las Comunidades Autónomas deberán adaptarse a lo establecido en el RGPD. En tal sentido, parece razonable que a corto o medio plazo se revise y adapte al RGPD (o se elabore una Ley vasca completamente nueva) la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

10. RÉGIMEN DE RESPONSABILIDADES Y SANCIONES: IDEA GENERAL. APLICACIÓN AL SECTOR PÚBLICO

Uno de los pilares de esta nueva regulación era dotar a la normativa (y, en particular, a las autoridades de control) de «poderes coercitivos más contundentes» con el fin de proteger los derechos y libertades de las personas físicas como consecuencia de los tra-

tamientos de datos personales. Detrás de todo ello está, sin duda, el avance imparable de la revolución tecnológica y el poder cuasi absoluto de las empresas de ese mismo ámbito que despliegan su actividad con el manejo y cruce de toda la información recuperada a través de los motores de búsqueda, de las redes sociales o de los correos electrónicos. Es algo muy conocido, más todo lo que esté por llegar en un escenario plagado de fuertes incertidumbres (Ver: Epílogo).

Con esa finalidad de fortalecer la aplicabilidad del nuevo marco normativo en esta materia, no quedaba otra opción que hacer el necesario hincapié en el poder sancionador. Y eso es algo que se recoge en los Considerandos 149 y siguientes del RGPD. Veamos un ejemplo.

CONSIDERANDO 148 RGPD

A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

ISBN: 978-84-7777-543-3

En todo caso, como anuncia el título del presente epígrafe, la pretensión de estas líneas es solo dar una idea general de esta problemática, entre otras cosas porque su aplicabilidad a las entidades del sector público se ve mediatizada por la regulación que se prevé en el PLOPD, dónde —a pesar del cambio cualitativo que implica el RGPD— en el ámbito sancionador se sigue el viejo patrón de la LOPD de 1999, con algunos matices.

Regulación en el RGPD

El Capítulo VIII del RGPD se enuncia del siguiente modo: «Recursos, responsabilidad y sanciones». De esa regulación nos interesa particularmente todo aquello que tiene que ver con la responsabilidad y el régimen de sanciones. Pero muy sucintamente ese Capítulo aborda los siguientes temas:

- Prevé el derecho que tiene todo interesado de presentar una reclamación ante la autoridad de control si considera que el tratamiento de datos personales aplicado infringe el presente Reglamento (artículo 77)
- De prevé, asimismo, el derecho a la tutela judicial efectiva en un doble sentido: contra una autoridad de control; y contra un responsable o encargado del tratamiento (artículos 78-79)
- Se regula la representación de los interesados (artículo 80) y la suspensión de los procedimientos (artículo 81)
- Se contiene una importante regulación relativa al derecho de indemnización y responsabilidad (artículo 82), de la que conviene destacar algunos extremos.
- Hay que tener en cuenta que este Capítulo VIII, sobre todo su artículo 83, reenvía a determinados «poderes» (con implicaciones obviamente sancionadoras) que ejercen las autoridades de control según el artículo 58 (por ejemplo, advertencias o apercibimientos).
- El artículo 83 establece lo que denomina como «Condiciones generales para la imposición de multas administrativas». Un precepto fundamental a partir del cual la legislación de los Estados miembros adaptará su régimen sancionador o lo impondrá en aquellos casos que no lo tuviera. Particularmente importante por lo que se dirá es el artículo 83.7 RGPD. Este precepto requiere asimismo una cita expresa.

DERECHO A INDEMNIZACIÓN Y RESPONSABILIDAD: EXTRACTOS (Artículo 82 RGPC)

1. Toda ***persona que haya sufrido daños y perjuicios materiales o inmateriales*** *como consecuencia de una* ***infracción del presente Reglamento tendrá derecho a recibir*** *del responsable o el encargado del tratamiento una* ***indemnización por los daños y perjuicios sufridos.***

2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

CONDICIONES GENERALES PARA LA IMPOSICIÓN DE MULTAS ADMINISTRATIVAS: EXTRACTOS (ARTÍCULO 83)

«1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta: (…)

ISBN: 978-84-7777-543-3

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía: (…)

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía: (…)»

LA PREVISIÓN PUNTUAL PARA LAS AUTORIDADES Y ORGANISMOS PÚBLICOS: Artículo 83.7 RGPD

7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, ***cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.***

Propuesta de regulación en el PLOPD

El Título IX del PLOPD trata del Régimen sancionador. Y muy brevemente nos interesa hacer mención a algunos de esos artículos, pero especialmente a la previsión recogida en el artículo 77 PLOPD, porque —de aprobarse en estos términos la futura LOPD— colocaría a las entidades del sector público en una posición similar a la que se encuentra actualmente la Administración Pública en el marco normativo vigente anterior al RGPD.

En términos generales, la citada regulación que se propone contiene los siguientes elementos:

- Sujetos responsables (artículo 70 PLOPD), donde entre otros se prevén los responsables y los encargados de los tratamientos, así como se afirma que al delegado de protección de datos no le será de aplicación el régimen sancionador previsto en ese título.
- Se tipifican las infracciones muy graves, graves y leves (respectivamente, artículos 72, 73 y 74)
- Se regula la interrupción de la prescripción (artículo 75) y el régimen de prescripción de las sanciones (artículo 78)
- También se recoge una regulación cobre sanciones y medidas coercitivas.
- Y, en fin, el artículo 77 del PLOPD establece un «régimen aplicable a determinadas categoría de responsables o encargados del tratamiento», con amparo en el artículo 83.7 RGPD. Y, dada su importancia para la Administración Local, es oportuno reproducirlo en su integridad, al margen de cómo quede realmente en la versión final tras su tramitación parlamentaria.

> Artículo 77 PLOPD: **Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.**
>
> 1. «El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

ISBN: 978-84-7777-543-3

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.

2. «Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 73 a 75 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.»

3. «Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos podrá proponer también la iniciación de actuaciones disciplinarias. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.»

4. «Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.»

5. «Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.»

«6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, ésta publicará en su página web con la debida separación las resoluciones en que se imponga una sanción a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.»

PARA SABER MÁS:

GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE DATOS DEL Artículo 29; 17/ES WP 253

DIRECTRICES SOBRE LA APLICACIÓN Y FIJACIÓN DE MULTAS ADMINISTRATIVAS A EFECTOS DEL REGLAMENTO 2016/679

11. OTRAS CUESTIONES. SITUACIONES ESPECÍFICAS DE TRATAMIENTO

Con carácter meramente telegráfico conviene poner de relieve algunas otras disposiciones que el RGPD encuadra como «situaciones específicas de tratamiento».

A tal efecto, se deberán tener en cuenta las siguientes previsiones:

— Tratamiento y libertad de expresión e información (artículo 85 RGPD) , lo que implica una obligación a los Estados miembros de conciliar la protección de datos personales con tal derecho fundamental, en particular en lo que se refiere al tratamiento con fines periodísticos y de expresión académica, artística o literaria.

ISBN: 978-84-7777-543-3

— En el artículo 86 RGPD se regula el **tratamiento y acceso a documentos oficiales**.
— Por su parte en el artículo 87 se prevé una **regulación del número nacional de identificación.**
— El artículo 89 prevé una serie de **garantías aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica y fines estadísticos.**
— El artículo 90 se ocupa de las **obligaciones de secreto**.
— Y, en fin, el artículo 91 tiene por objeto las «**normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas**».
— Particular importancia tiene la previsión del artículo 88, sobre **tratamiento en el ámbito laboral,** que cabe entender plenamente aplicable a las relaciones de empleo en el ámbito del sector público.

Artículo 88 RGPD: TRATAMIENTO EN EL ÁMBITO LABORAL

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

> 3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

En este sentido es de notable importancia la propuesta normativa recogida en la Disposición adicional decimoquinta del PLOPD que tiene por objeto una serie de «disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público».

> *Disposición adicional decimoquinta. Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.*
>
> *1. Los tratamientos de los registros de personal del sector público se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento (UE) 2016/679.*
>
> *2. Los registros de personal del sector público podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines.*
>
> *3. De acuerdo con lo previsto en el artículo 18.2 del Reglamento (UE) 2016/679, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 del citado reglamento, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.*

Asimismo, por lo que afecta a la Transparencia publicidad activa y al derecho de acceso a la información pública, es importante tener en cuenta lo recogido en la disposición adicional segunda del PLOPD que, en materia de protección de datos reenvía a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, a lo establecido en el RGPD y también a lo que regule la LOPD. Esta referencia debe entenderse exten-

ISBN: 978-84-7777-543-3

siva a lo establecido en la Ley 19/2014, del Parlamento de Cataluña, de transparencia, acceso a la información pública y buen gobierno.

DOCUMENTO RECIENTE DE LA AEPD:

Listado de cumplimiento normativo para facilitar la adaptación al RGPD

https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_04_13-ides-idphp.php

Epílogo

El futuro de la protección de datos en un entorno de revolución tecnológica

«La era del algoritmo marca el momento en que la memoria técnica ha evolucionado para almacenar no solo nuestros datos, sino también algunos patrones del comportamiento más sofisticado, desde el gusto musical hasta nuestros grafos sociales. En muchos casos, ya nos estamos imaginando sincronizados con nuestras máquinas».

(Ed Finn, *La búsqueda del algoritmo. Imaginación en la era de la informática*, Alpha Decay, p. 336)

«Puede que llegue el momento, quizás más pronto que tarde, de que la pregunta sobre la ética de los algoritmos deba plantearse con respecto a la inteligencia artificial en evolución o, incluso, deba dirigirse a esa mente-máquina. De momento, aún es esencialmente una pregunta para los seres humanos que escriben los algoritmos»

(Thimothy Garton Ash, *Libertad de palabra. Diez principios para un mundo conectado*, Tusquets Editores, 2017, p. 494).

ISBN: 978-84-7777-543-3

No parece exagerado bajo ningún punto de vista hablar de que **la digitalización acelerada de la sociedad contemporánea nos ha conducido irremediablemente a una suerte de panóptico digital**, donde el nivel de exposición de lo que hacemos, pensamos o, incluso, queremos, es más que evidente. El filósofo Byung-Chul Han trató en diferentes obras esa noción de «panóptico digital», concepto que, importado de Bentham, construye precisamente en uno de sus primeros trabajos traducidos al castellano (*La sociedad de la transparencia*, Herder, 2013). Pero en alguna obra posterior este mismo autor llegó incluso a hablar de la obsolescencia del concepto de protección de datos, algo que vinculaba con la exposición en la red de todo tipo de datos e informaciones sobre nosotros mismos. Y concluía: «Este descontrol representa una crisis de libertad que se ha de tomar en serio» (*Psicopolítica,* Herder, 2014).

Tal como se ha expuesto, la necesidad objetiva de protección de los derechos fundamentales de las personas físicas **en un mundo cada vez más digitalizado y en el que el «algoritmo» se ha convertido en nuestro inseparable compañero, la regulación que lleva a cabo el RGPD hay que entenderla precisamente como medio de salvaguardar una protección suficiente de los datos personales** con el objetivo último de que, efectivamente, nuestra libertad no se vea menoscabada, aunque amenazada lo está y mucho.

Otro filósofo, como es Paul Virilio, hace algunos años dio probablemente en la diana: «Las tecnologías no son otra cosa más que prótesis y pensar la libertad con respecto a las prótesis resulta algo absolutamente nuevo» (*La Administración del miedo,* Pasos Perdidos, 2012). Sin embargo, como ya anticipaba este mismo autor, **la velocidad de los hechos ha desbordado al Derecho,** más aún en este complejo campo de la digitalización, puesto que «el derecho del más rápido es el origen del derecho del más fuerte». Y es también en esta clave en la que se debe interpretar el alcance del RGPD y el propio espíritu o sentido que lo anima.

Creo, aunque sea reiterar algo ya expuesto, que si bien **la normativa europea** llega probablemente tarde, **al menos intenta hacer frente a todo ese conjunto imprevisible de riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas.** Pero en estas páginas **interesa destacar en qué medida todo ello afecta o afectará a la Administración Pública y a los entes de su sector público.** A las personas físicas sin duda que lo hará. En efecto, si bien esa mirada debe ser predominante, no es menos cierto

que si se prescinde del eje central en el que se basa el RGPD (la protección de los derechos fundamentales y libertades públicas de la ciudadanía), el sector público no cubrirá cabalmente las expectativas que la nueva regulación tiene puestas en su aplicación.

Todos esos «riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas» (artículo 24.1 RGPD) irán inevitablemente siendo cada vez mayores conforme la revolución tecnológica avance de forma inexorable. Ciertamente, se puede pensar que nos encontramos en un estadio avanzado del proceso de digitalización, pero en verdad todos los estudios sobre prospectiva del desarrollo de tal proceso de la revolución tecnológica nos conducen a escenarios de mucha mayor intromisión o de amplia incertidumbre y, en cualquier caso, a una sociedad en la que «las máquinas» desempeñarán buena parte de las tareas actuales que despliegan en estos momentos las personas (con la afectación al mercado de trabajo y, especialmente, a los perfiles profesionales que se demandarán).

Comienza a emerger, en los ámbitos profesionales y se traslada sin duda a la Administración Pública, una necesidad imperiosa de controlar los datos. Como ha sido expuesto por Richard y Daniel Susskind, los profesionales «se encuentran con que conjuntos enormes de datos, relacionados con sus pacientes, estudiantes y clientes pueden aportar ideas muy útiles» (*El futuro de las profesiones, Cómo la tecnología transformará el trabajo de los expertos humanos,* Tell, 2017). Ese campo de análisis predictivo, de rastreo de datos o de aprendizaje automatizado, en el que al fin y a la postre consiste el *Big Data*, conlleva la aparición de ámbitos profesionales nuevos (analistas de datos o «algoritmistas»), pero a su vez pone el foco sobre los derechos fundamentales de las personas, lo que requiere un control de esos datos y unas medidas de seguridad apropiadas. Pero también, como en su día resaltaron Mayer-Schönberger y Cukier *(Big Data. La revolución de los datos masivos.* Turner, 2013)*,* hay una necesidad imperiosa de que las personas controlen por sí mismas el uso que hagan de sus datos, debiéndose incrementar las medidas de autocontrol, algo no precisamente fácil en una sociedad completamente interconectada.

Pero eso solo es una parte del problema. El desarrollo de la inteligencia artificial en las próximas décadas abre incógnitas enormes. Jerry Kaplan en un sugerente ensayo (*La inteligencia artificial. Lo que todo el mundo debe saber,* Tell, 2017), abre un escenario de preguntas sobre diferentes ámbitos hasta cierto punto inquietantes, hasta plantearse en su recorrido argumental la *idea de singularidad*, lo que implica que en

ISBN: 978-84-7777-543-3

algún momento temporal «las máquinas serán suficientemente inteligentes como para poder rehacerse y mejorarse a sí mismas, lo que producirá una explosión de inteligencia». Para Ray Kurzweil es el destino inexorable al que conduce la revolución tecnológica, para otros, como Fukuyama, ese desarrollo es peligroso para la humanidad.

La tensión entre humanismo y transhumanismo parece palparse. Como ha expuesto Luc Ferry, estamos en pleno proceso de superación del «ideal terapéutico» que tenía como objeto curar o reparar, y vamos así camino del «ideal de aumentar o perfeccionar». Y en ello, como afirma también este mismo autor (*La revolución transhumanista,* Alianza Editorial, 2017), juega un papel central el acrónimo NBIC (nanotecnología, biotecnología/informática-Big Data/Conocimiento aplicado a la Inteligencia Artificial). Todo ello abre, en efecto, un manejo múltiple y cruzado de datos, pero especialmente un horizonte de problemas éticos de primera magnitud, que en estos momentos no pueden ser tratados. Ya lo dijo en su día Jean Stane, en su libro *Les clés du futur* (citado en la obra de Luc Ferry), «si fuera posible realizar una máquina que sea en todo punto equivalente a un ser humano, las consecuencias serían asombrosas y terroríficas». Frente a tesis alarmistas, también se cruzan tesis de optimismo evidente, cuyo lema es que «las nuevas tecnologías podrán resolverlo todo». Probablemente, como todo en la vida, en el término medio estará la virtud. Pero los riesgos están presentes, siendo cada vez mayores, y el RGPD los recuerda una y otra vez con su sistema preventivo.

No obstante, aunque no haya acuerdo unánime al respecto sobre este punto (unas personas hablan de tercera y otras de cuarta revolución), lo cierto es que **se ha inaugurado con fuerza lo que puede calificarse como un largo período de revolución tecnológica en la que la digitalización (y el dato, como núcleo) está (y estará) en el centro de todo este proceso**. La economía se ha digitalizado y el RGPD no pretende obstaculizar ese desarrollo, sino ordenarlo, que es cosa bien distinta, en el sentido de garantizar la libre circulación de datos, pero enmarcando ese proceso en una serie de reglas bien definidas.

El modelo se ha ido desarrollando y asentando paulatinamente, tomando como apoyo fuerte que se trataban de «servicios gratuitos» (ofertados por las grandes compañías tecnológicas) a cuenta, tal como se ha dicho, de entregarles o hacer jirones nuestra privacidad. A partir de esos presupuestos, la práctica totalidad de la humanidad digitalizada ha «ofrecido» sus datos (y, por tanto, sus preferencias, su vida e, incluso, sus expectativas) a tales compañías, que comercializan sin rubor

ni límite alguno (al menos hasta ahora) con tales datos. La «mediación algorítmica», como ya advirtió tempranamente Evgeny Morozov, tiene sus peligros (*La locura del solucionismo tecnológico*, Katz, 2013).

Pero tales «peligros», como también resalta el propio RGPD tanto en sus Considerandos como en el articulado, aparte de ser inciertos, todo el mundo es plenamente consciente (o al menos así se presume) de que irán creciendo cuantitativa y cualitativamente con el paso del tiempo. Y para ello la Administración Pública debe prepararse convenientemente, tanto dotándose de medios «técnicos y organizativos» adecuados para hacer frente a tales incertidumbres o peligros, como especialmente en invertir en la construcción de ese modelo de gestión de protección de datos basado en el enfoque de riesgos. No es una cuestión menor, tampoco incidental o de cumplimiento normativo, es sencillamente existencial: la Administración Pública está al servicio de la ciudadanía y debe salvaguardar en todo momento los derechos fundamentales y libertades públicas de las personas físicas, en particular en todo los que afecta a la protección de datos personales. Y para ello tal vez sea oportuno llevar a cabo unas sucintas reflexiones sobre prospectiva.

Si tomamos, por ejemplo, los estudios de prospectiva que tienen por objeto el impacto de la revolución tecnológica sobre el empleo tal vez nos aporten algunas aproximaciones que puedan tener interés al objeto de estas líneas. Así en un reciente estudio de PwC editado en el Reino Unido (*Will robots really steal our jobs? An international analysis of the potencial long term impact of automation*, 2017), se determina que la revolución tecnológica hoy en día en marcha tendrá tres grandes oleadas o etapas. A saber:

- La primera oleada es la «digitalización» propiamente dicha. Es una etapa en la cual estamos hoy en día inmersos. También las Administraciones Públicas que deben cumplir, entre otras cosas, las exigencias de la Ley 39/2015, de 1 de octubre, de procedimiento administrativo común de las administraciones públicas.
- La segunda oleda es la de «automatización», y que se desarrollará en torno a 2025, momento en el que las máquinas llevarán a cabo una parte importante de las tareas y en el que habrá que estar vigilantes para evitar que esos cambios tecnológicos de magnitudes considerables puedan afectar a los derechos y libertades de las personas físicas en el tratamiento de sus datos personales. En esta fase, encontrarán pleno sentido muchas de las

ISBN: 978-84-7777-543-3

previsiones recogidas en el RGPD, especialmente aquellas dirigidas a «la protección desde el diseño y por defecto», así como, en su caso, la evaluación de impacto y la consulta previa. Para ese momento las Administraciones Públicas deberían tener plenamente implantado y a pleno rendimiento el sistema institucional y de gestión de protección de datos personales que exige el RGPD. Ello garantizaría que las afectaciones pudieran ser menores o, cuando menos, controladas.

— **Y la tercera oleada, sin duda la más crítica, en la que las incertidumbres se multiplicarán, es la de la aplicación de la Inteligencia Artificial al ámbito de las Administraciones Públicas y en lo que respecta también a la protección de datos personales.** Se estima que, temporalmente, esta etapa se puede producir **en torno a los años 2030-2035** (al menos así lo confirman los diferentes estudios de prospectiva: ver, por ejemplo: *50 Estrategias para 2050*, Fundación Telefónica/Prospektiker: https://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/636/), donde los cambios cualitativos pueden ser de una dimensión desconocida hasta entonces. Veremos si el marco normativo diseñado en el RGPD es suficiente para enfrentarse a un reto de tales características, que impregnará sin duda todo o gran parte del actuar de las Administraciones Públicas como prestadoras de servicios, que en no pocos casos ya los harán las maquinas «inteligentes» y no las personas.

Sin duda la revolución tecnológica se caracteriza por la importancia que los *datos* adquieren en la propia economía. Se ha dicho así que los datos son el petróleo de la economía digital, pero eso no es verdad, pues —tal como afirma Franklin Foer— «los datos son infinitamente renovables, no son finitos como el petróleo». **La amenaza de los datos a la intimidad y al resto de derechos y libertades es, hoy en día, obvia.** Uno de los principales asesores de una las grandes empresas monopolísticas de Internet, **Eric Schmidt**, lo reconocía con toda crudeza: «***Sabemos dónde estás. Sabemos dónde has estado. Podemos saber más o menos lo que estás pensando***».

Los datos empujarán el crecimiento económico, no cabe dudar de ello. Pero también son un desafío real y tangible a la privacidad, aunque ya hay quien dude que en la era de Internet y de las redes sociales tal derecho a la intimidad tenga vigor alguno. **La solución**, como apunta

Luc Ferry en su recomendable obra citada al inicio de este trabajo, pasa inevitablemente por la *regulación.* Habrá que seguir y persistir en esa línea.

Por mucho que se empeñen los diletantes y resistentes, especies que abundan precisamente en el ecosistema público, en los próximos años la revolución tecnológica transformará en viejas muchas de las prácticas y formas de actuar que están insertas en el funcionamiento cotidiano de las Administraciones Públicas, también (aunque no solo) en lo que afectan a la protección de datos personales. Esa revolución tecnológica exigirá nuevos perfiles profesionales en la Administración Pública, de los que la figura del Delegado de Protección de Datos es un mero anticipo. No cabe descartar que, al igual que en otras organizaciones, el sector público se deba dotar de un buen número de tecnólogos especialistas en algoritmos, aquí de nuevo surge la plétora de demanda de profesiones vinculadas al acrónimo inglés STEM (Ciencia, Tecnología, Ingeniería y Matemáticas). Si se quiere realmente reforzar la protección de datos personales y los derechos fundamentales y libertades públicas, el papel de esos «tecnólogos» será muy importante en el sector público, también en materia de protección de datos.

Pero, como se viene insistiendo, ello requerirá un cambio cultural y organizativo de magnitudes considerables, si bien hoy por hoy nada de esto parece advertirse en el funcionamiento de nuestras adormecidas y tradicionales organizaciones públicas, sino más bien lo contrario (la regla es, en efecto, la quietud y el funcionamiento estandarizado).

Por tanto, los efectos más profundos de la revolución tecnológica sobre la Administración Pública (así como sobre el ámbito empresarial y económico), también sobre la protección de datos personales, vendrán de la mano del binomio robotización/Inteligencia artificial, ambos términos complementarios o indisolublemente unidos. Una vez más cabe recurrir a las palabras de Luc Ferry, pues parece obvio que la nanotecnología, la biotecnología, la informática de *Big Data* y el Conocimiento vinculado a la Inteligencia Artificial, «van a generar más cambios en los próximos cuarenta años que en los cuatro mil anteriores», como dice ese autor.

Y esos profundos cambios abrirán un sinfín de retos, pero también se inaugurará un tiempo de tensiones extraordinarias. El transhumanismo radical produce vértigo. Realmente esa pretendida simbiosis entre el hombre y la máquina solo conduce al «posthumanismo»

ISBN: 978-84-7777-543-3

o al «antihumanismo». Ciertamente, si atendemos al juicio fundado de dos científicos consagrados del campo de la IA, López de Manteras Badía y Meseguer González (*Inteligencia Artificial,* Catarata, 2017), ese horizonte de fusión entre «hombre y máquina» está aún muy lejano, de momento hay que apostar por la complementariedad y no por la sustitución. La IA débil o especializada (la que realiza *tareas* que requieren inteligencia) ha tenido un fuerte desarrollo, mientras que la IA fuerte o general (la que permite *replicar* la inteligencia humana mediante máquinas) está lejos de alcanzarse. La explicación, a juicio de estos autores, es muy clara, pues consiste *en la dificultad de dotar a las máquinas de conocimientos de sentido común*. Aún así, los riesgos están allí, por lo que todo este mundo abre un amplio abanico de problemas éticos de no fácil solución y que, más temprano que tarde, habrá que afrontar.

Pues bien, todo esto por fuerza (o por la naturaleza de las cosas) terminará afectando al sector público, además de forma profunda e inevitable. Y asimismo impactará sobre la protección de datos personales, que estará en el centro del problema. Pues no cabe olvidar que esta revolución tecnológica, como todas revoluciones industriales anteriores, comportará también una suerte de *destrucción creativa*, en términos del insigne economista Schumpeter (*Capitalismo, socialismo y democracia,* vol. I., Página Indómita, 2015).

La revolución tecnológica puede encuadrarse en ese esquema schumpeteriano, pero con algunas singularidades. Bien es cierto que es, como dijo el autor austriaco, un ejemplo de «revolución incesante con acontecimientos discontinuos», superada una y otros por lapsos de relativa calma (algo que en el caso de la revolución tecnológica es más difícil de justificar, pues el proceso es de aceleración constante). Pero lo relevante es que ese proceso de destrucción creativa —como sancionó Schumpeter— es la clave del capitalismo y conlleva un fenómeno de «destrucción ininterrumpida de lo antiguo y una creación continua de elementos nuevos».

En ese proceso de «destrucción creativa» que ya está llamando a nuestra puerta, el problema que tiene la Administración Pública para llevar a cabo esos ajustes tan drásticos que el nuevo escenario tecnológico anuncia, también en el ámbito de protección de datos personales, radica principalmente en su enorme rigidez estructural y su anquilosamiento normativo. Pero este último elemento, el anquilosamiento normativo, al menos por lo que respecta a la protección de datos personales, ha sido removido drásticamente

por el «legislador europeo»: la plena efectividad del RGPD abre un sinfín de retos aplicativos a las Administraciones Públicas a los que deben inexorablemente enfrentarse, puesto que la revolución tecnológica alterará la esencia de las cosas y en todo este proceso, la proteccion de datos personales dejará de estar en la perfieria de las políticas públicas para situarse en el epicentro de muchas de ellas. Algo que el paso del tiempo irá confirmando.

SMART CITY Y PROTECCIÓN DE DATOS:

«¿Y qué significa realmente la retórica en torno a la smart city o ciudad inteligente? Si se lee más de cerca, quiere decir que nuestra infraestructura urbana será entragada a un grupo de empresas tecnológicas (desde luego no muy propensas a la transparencia) que luego la gestionarán como mejor les parezca, lo que hará casi imposible remunicipalizarlas más adelante»

*(Evgeny Morozov, **Capitalismo Big Tech**, Enclave, 2018, P. 269).*

ÉTICA Y REVOLUCIÓN TECNOLÓGICA:

Un documento muy reciente (9 abril 2108), sobre problemas éticos y revolución tecnológica es: *A **Statement** on Artificial Intelligence, Robotics and «autonomous» systems by the European Group of Ethics and Science in New Technologies*: http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

IVAP
HERRI ARDURALARITZAREN
EUSKAL ERAKUNDEA

Erakunde Autonomiaduna
Organismo Autónomo del
EUSKO JAURLARITZA
GOBIERNO VASCO