Junta de Castilla y León

eclap

JORNADA

APLICANDO LA NUEVA NORMATIVA SOBRE PROTECCIÓN DE DATOS

VALLADOLID, 17 DE OCTUBRE 2018

PROBLEMÁTICA EN LA APLICACIÓN DEL RGPD

Miguel Ángel del Barrio Moreno
Delegado de Protección de Datos
Diputación de Segovia

Junta de Castilla y León

eclap
Escuela de Administración Pública de Castilla y León

PROBLEMÁTICA EN LA APLICACIÓN DEL RGPD

Miguel Ángel del Barrio Moreno

Técnico Jurídico de Asuntos Sociales y Deportes.
Delegada de Protección de Datos.
Diputación de Segovia.

INDICE

ESTE DOCUMENTO...

...identifica y explica los principales problemas con los que se pueden encontrar las administraciones públicas, en especial las entidades locales, a la hora de adaptar su actividad al Reglamento General de Protección de Datos (en adelante RGPD), al mismo tiempo que se proponen algunas fórmulas para evitarlos, minimizar sus efectos desfavorables y sobreponerse a ellos.

El trabajo parte de la experiencia profesional de la implantación del RGPD en la Diputación de Segovia, desde la perspectiva del Delegado de Protección de Datos (en adelante DPD) de la Institución Provincial. Expone, por tanto, una visión subjetiva de la puesta en práctica de la Ley, sin que ello deba ser, necesariamente, de la manera que consta en este documento.

Es un instrumento eminentemente práctico que tiene por finalidad, desde la humildad, servir de referencia a los agentes que tienen encomendada la tarea de liderar, impulsar y acometer la aplicación del RGPD. Una guía también anímica frente a las dificultades en su aplicación.

Espero que esta información les sea de utilidad.

UNA CONSIDERACIÓN PREVIA

"Estamos cambiando radicalmente las relaciones entre la administración pública y los ciudadanos. Queremos que la administración pública se mueva al mismo ritmo y hable el mismo idioma que sus usuarios. El enfoque de muchas administraciones todavía se centra demasiado en obligaciones y procedimientos y demasiado poco en la mejora de la calidad de vida de los ciudadanos." Marianna Madia, ministra italiana de Administración Pública y Simplificación, Conferencia de la Comisión Europea, 1 de octubre 2014.

Me parece oportuno empezar con esta declaración, tan recurrente en muchas exposiciones sobre la calidad de los servicios públicos, puesto que representa el cambio de paradigma al que asistimos en el sector público. Una perspectiva rupturista, sobre todo de mentalidad, que exige nuevas formas de hacer, de pensar, de actuar, de escuchar, de posicionarse... en las relaciones con los ciudadanos. Las instituciones públicas deben –debemos– poner el foco en los receptores de nuestra acción y acercar la gestión pública a las personas. Detectar los cambios en las necesidades y preferencias de los princípiales consumidores de los servicios públicos, y adaptarnos a ellas.

Esta transformación ya ha comenzado. Avanza a un ritmo vertiginoso a cuestas de las nuevas tecnologías que lo aceleran aún más para tratar de acoplar la gestión pública a la eficacia y calidad que demanda la sociedad actual. En consecuencia, la administración debe adaptarse a esa velocidad y dar respuestas a las preocupaciones que ello pueda generar, **ser más garantista y protectora en coherencia con la utilización masiva de datos y de información** que conlleva la participación y la transparencia en estos tiempos que corren. (Ver considerando sexto RGPD). Ahí está la clave, en facilitar la vida administrativa a las personas a través de la transformación digital, a la vez que se les transmite confianza mediante la provisión de las medidas de seguridad precisas. En este sentido, el rol de la administración será el de

adoptar una posición de proactividad y dotar de seguridad al sistema desde el diseño *("privacy by design"),* así como tratar sólo los datos que sean necesarios, durante el menor tiempo posible y con el mínimo acceso *("privacy by default").* (Ver artículo 25 RGPD).

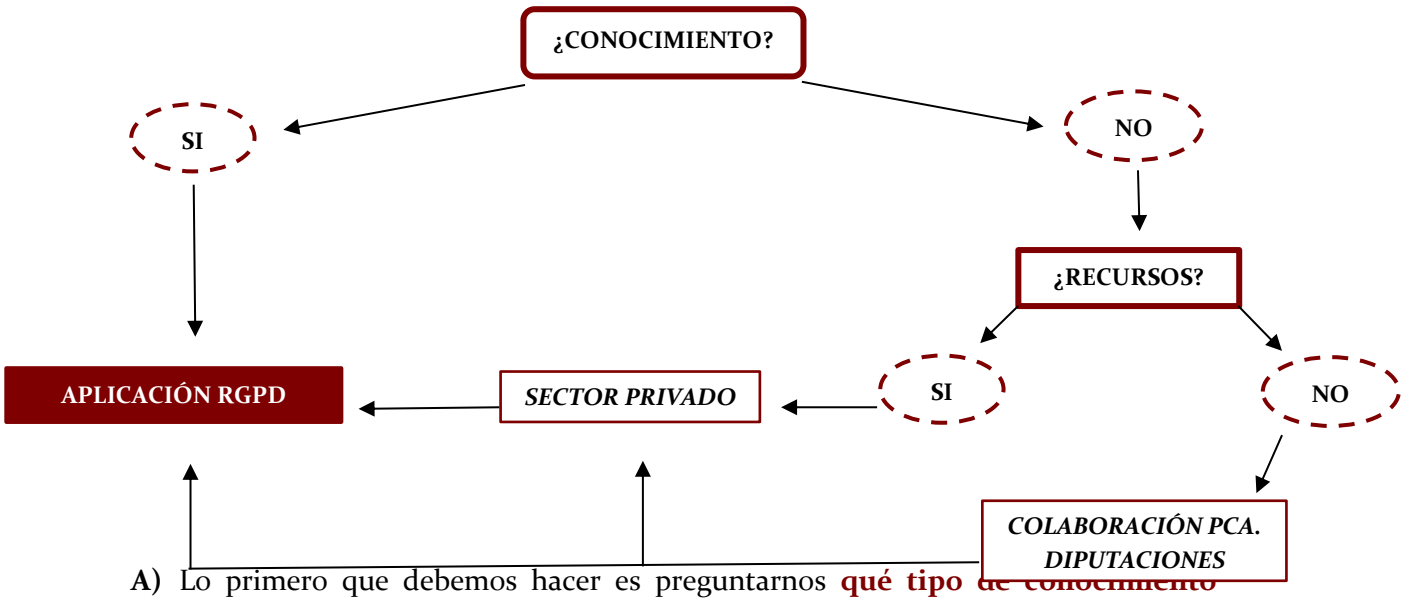
Pero también, en relación a este cambio de paradigma al que nos referimos, los ciudadanos han dejado de ser meros destinatarios de servicios y piden que se presten con calidad. Ya *"hablan"* con la administración, exigen de aquella una determinada actitud frente a la antigua visión gerencialista o burócrata de proporcionar servicios con la única condición de que se hiciese con sujeción al procedimiento legal preestablecido. En este sentido, **las personas conocen sus derechos, reclaman su ejercicio y esperan que se adopte una posición proactiva en el acceso a los mismos.**

Así, pues, debemos ser conscientes de ello a la hora de ponernos manos a la obra. No sólo es cambiar los formularios que lleven datos personales, ni publicar el registro de actividades de tratamiento, ni la disposición de canales sencillos y accesibles para el ejercicio de los derechos, no exclusivamente, es algo más. Es un cambio en la cultura de las organizaciones públicas, de sus empleados, una nueva filosofía en las relaciones con los administrados. Esto es lo que motiva esta nueva manera de proceder, en general, que ahora afecta al tratamiento de los datos personales.

1. CONOCIMIENTOS Y RECURSOS

El conocimiento técnico, entendido como aquel relacionado con el área o el proceso de trabajo del individuo, es el principal activo de las organizaciones. Es indispensable para su progreso y la consecución de sus objetivos. Este tipo de conocimiento se va adquiriendo a través de un proceso académico, de la acción formativa específica, del continuo reciclaje, del intercambio de información y, por supuesto, de la propia experiencia. Cuanto más grande es la organización mayor variabilidad de ese conocimiento técnico existirá en ella; en otras palabras, más perfiles profesionales con diferente *expertise* habrá.

Lo que ocurre es que no todas las administraciones tienen la posibilidad de contar con todos los conocimientos precisos para acometer los diferentes proyectos que les exige el ordenamiento jurídico en el marco de sus competencias. En estos casos, cuando el grado de especialización técnica requerido no se encuentre en la organización, será preciso acudir al mercado para suplirlo ante la falta de medios propios. El problema se agrava cuando además de los conocimientos precisos para su abordaje, tampoco se cuenta con los recursos económicos para su adquisición en el sector privado, en cuyo caso, deberán buscarse otras fórmulas de cooperación o de actuación colaborativa con entidades afines con mayores recursos. Veamos, pues, **SOLUCIONES** al **problema del conocimiento** en la aplicación del RGPD, desde el abordaje de estos **tres supuestos**.



A) Lo primero que debemos hacer es preguntarnos **qué tipo de conocimiento técnico se exige en el RGPD** para su adecuado cumplimiento. El perfil es complejo: necesitamos ingenieros que conozcan la normativa, y juristas con conocimientos tecnológicos e informáticos. Suele ser más fácil que se dé lo primero, pero tampoco es lo habitual. Sin ir más lejos, con respecto al DPD, ya el RGPD habla de un cierto grado de especialización. Según el artículo 37.5 RGPD, *"el DPD será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y* ***a su capacidad para desempeñar las funciones indicadas en el artículo 39.***" Se refiere a un jurista con conocimientos en materia de protección de datos, pero además que tenga capacidad para el

desempeño de las funciones del artículo 39, lo que implica conocer todas las obligaciones a cumplir por parte del responsable y encargado del tratamiento, incluidas las medidas de seguridad con alto contenido tecnológico. Lo más probable es que las administraciones no cuenten con este perfil profesional, al menos ya en plantilla con anterioridad a la aplicación del RGPD. El propio Reglamento es consciente de ello, de ahí que no pida la previa acreditación como DPD. Proceder a su creación en la RPT y a su posterior selección pública se antoja complicado y para nada ágil. Además, todo lo que suponga un incremento en el gasto de personal, es algo de lo que no se quiere oír hablar en la administración pública, sobre todo en la local en la que el capítulo I es uno de los más abultados.

Así, pues, la **solución** ante el problema del conocimiento para el desarrollo del proyecto de adecuación, pasa por **aprovechar las sinergias de la propia organización**, en cuanto a la utilización para este fin de los perfiles ya predispuestos, separar parte de su dedicación a ello y formarlos. De esta manera se ha hecho en la Diputación de Segovia, en la que se ha optado por un sistema mixto en la que la figura del DPD es ocupada por dos profesionales, a saber: un técnico jurídico con conocimientos básicos en protección de datos y un ingeniero en telecomunicaciones que venía ya dedicándose a la política de seguridad en la utilización de medios electrónicos, el Esquema Nacional de Seguridad (ENS). Puesto que la Agencia de Protección de Datos no prevé la inscripción de dos DPD sobre una misma organización, la fórmula adoptada se formalizó mediante la asignación de un DPD (el jurídico) a la Diputación de Segovia como entidad propia, responsable y encargada de tratamientos, y del otro (el ingeniero) a los organismos autónomos dependientes de ésta, de esta forma se salvó el escollo de la inscripción del DPD, aunque su trabajo es conjunto, coordinado y solidario con respecto a las funciones encomendadas a esta figura, para la Diputación y también para los organismos vinculados a ésta.

En mi opinión, lo ideal hubiese sido crear una unidad administrativa dentro de la organización que se encargase de todo aquello concerniente a la modernización, innovación y transparencia de la administración, dotada de personal administrativo y técnico, tanto de corte jurídico como informático, y que desde esa unidad se llevasen a cabo las tareas de adaptación al RGPD encomendadas al

responsable y encargado del tratamiento, e incluso se diese también cobertura a los municipios de la provincia, y que de ahí saliese, aunque de manera independiente, la figura del DPD. No obstante, debemos ser conscientes de las limitaciones presupuestarias, ser eficientes y optar por la asignación de tareas entre los empleados públicos existentes, teniendo en cuenta, claro está, la incompatibilidad de funciones sobre todo en lo relativo al DPD.

B) Como dije al principio del epígrafe, pudiera suceder que por el alto grado de especialización técnica que exige la aplicación del RGPD, **deba acudirse al sector privado mediante un contrato de servicios,** al menos, para el acometimiento de parte del proyecto. Es otra opción válida que prevé el propio Reglamento. Diputación de Segovia, ha recurrido a los servicios de una consultora, *Instituto CIES*, para que le acompañe en la implantación del RGPD, sobre todo en la parte del análisis de riesgos, de las medidas de seguridad, de índole más técnica y compleja, y para la certificación de un sistema de información. También es favorable obtener la visión de un tercero externo, pues buena parte del éxito dependerá de esa evaluación. Pero ello no significa la completa externalización del proyecto, lo cual, a mi juicio, sería un error, al igual que la contratación de una empresa que haga las veces de DPD. La seguridad es un proceso interno de la organización. Debe impulsarse, liderarse y controlarse desde dentro. Nadie mejor que los integrantes de la administración conocen las vicisitudes que la comprenden, y nadie mejor que ellos sabrán qué actividades de tratamiento de datos realizan, con qué finalidad, que prácticas son susceptibles de mejora, cómo inculcar la cultura de la protección de datos entre los empleados, etc... Sin embargo, como digo, **donde no lleguemos, debemos completar el conocimiento con el de una empresa especializada** del sector, y formar un equipo en el ámbito de una economía colaborativa público-privada.

C) El tercer problema relativo al conocimiento específico, es que éste no exista, ni **tampoco se tengan los recursos suficientes para su adquisición en el mercado**. Esto ocurre sobre todo con las entidades locales pequeñas, en las que los medios personales reúnen los perfiles más comunes de la práctica administrativa, pero se echan en falta otros necesarios para la plena satisfacción

de los nuevos mandatos normativos. La verdad es que últimamente asistimos a una vorágine legislativa, que incluye una serie de obligaciones cuyo cumplimiento se antoja altamente complicado por parte de determinadas administraciones públicas debido a la falta de medios para ello. Lo vimos con las exigencias de la información pública de la Ley de transparencia, con la rendición de cuentas trimestral incluida en la Ley de Sostenibilidad financiera, con la creación de los registros electrónicos dispuestos en la Ley 39/2015 cuya efectividad se ha tenido que prorrogar, y ahora con la aplicación del RGPD.

En estos casos, no queda otra que establecer **mecanismos de cooperación pública** de tal manera que las administraciones grandes tiren de las pequeñas. Acudir a **economías de escala** y centralizar el problema pero repartiendo la solución, esto es, diseñar medidas en una organización para todas las demás. En este sentido, las **Diputaciones** cobran una importancia vital para la adaptación de la actuación de los pequeños municipios al RGPD, en virtud de lo establecido en el artículo 36 de la Ley de Bases del Régimen Local (ver artículo 36 LBRL). Lo que no tiene sentido es que si en España existen más de 8.000 Ayuntamientos, todos ellos inviertan recursos, si es que los tienen, cuando en todos ellos la casuística y las medidas a implementar son muy parecidas. Seamos eficientes y acudamos a nuestro hermano mayor, que para esto está. La Diputación de Segovia, apoya a los municipios en materia RGPD desde el departamento de *"Asesoramiento a Municipios"* donde se ubica el DPD para su asesoramiento, desde donde se llevarán a cabo los trámites para la contratación de una empresa que se encargue de la aplicación del RGPD en toda la provincia, y desde donde se fomenta la acción formativa en este ámbito. Pero ojo, esto no significa que los pequeños municipios se desentiendan del problema, –tened en cuenta que son los responsables del tratamiento de sus datos– sino que desde las Diputaciones se les apoye para minimizar los efectos negativos de su abordaje.

Al igual que las Diputaciones para los municipios, podríamos decir lo mismo de las Comunidades Autónomas respecto a aquellas y a los Ayuntamientos grandes, así como del Gobierno Estatal, respecto a todas ellas a través de la Agencia de Protección de datos.

2. FECHA LÍMITE

PROBLEMA: Vamos tarde. En general, la mayor parte del sector público no ha cumplido el RGPD el día de su aplicación, el **25 de mayo de 2018**. Pese a la *vacatio legis* de dos años desde su aprobación, nos ha pillado el toro. La verdad es que considero que ha sido un problema de todos, no sólo de los propios responsables y encargados del tratamiento, puesto que la mayor parte de los impactos sobre el RGPD (formación, publicidad y concienciación) han llegado los meses previos a la aplicación, e incluso después.

SOLUCIÓN: Sin prisa pero sin pausa.

"No pasa nada" si a la fecha no cumplíamos en su totalidad el RGPD. Esta circunstancia no es grave en el ámbito público, o al menos no más que el hecho de no estar haciendo aún, a día de hoy, actuaciones tendentes a su cumplimiento, aunque tampoco a esta fecha cumplamos en su totalidad el RGPD. **Lo importante es llegar**. Que la adaptación sea progresiva pero constante, ininterrumpida y proporcional a la tipología de actividades de tratamiento.

3. PLANIFICACIÓN

El **PROBLEMA** de no cumplir en plazo, además, es la **precipitación en el acometimiento del RGPD**. Las prisas no son buenas, y el ir contrarreloj para cumplir cuanto antes las obligaciones del RGPD puede suponer un riesgo para su eficacia al no disponer de una planificación adecuada. Ésta, es la práctica habitual en un sector público en el que la mayor parte de las ocasiones trabajamos día a día apagando los fuegos administrativos que surgen de las necesidades cotidianas, sin pararnos a pensar en la **visión** y en una **estrategia** para su consecución.

"Nunca existe un buen viento para el barco que no conoce su destino" (Seneca)

SOLUCIÓN: Tan importante es el "*qué*" como el "*cómo*". En este sentido, pese a la premura de la aplicación del RGPD, es importante **tener definido un modelo práctico**, una hoja de ruta que nazca de la realidad de la propia organización, que vaya de menos a más y que aproveche lo que ya se tiene para no empezar de cero.

La clave para conseguir el objetivo final, es fraccionarlo en mini objetivos e ir cumpliendo cada uno de ellos.

Propuesta de hoja de ruta para la aplicación del RGPD en la Diputación de Segovia.* ***Fuente: Instituto CIES.*

Henry Ford: "Nada es especialmente difícil si lo divides en trabajos pequeños"

A veces los árboles no nos dejan ver el bosque, de tal manera que ya tenemos cosas hechas, o existen ámbitos en los que es más fácil implantar las medidas, y por los que haya que empezar.

Por ejemplo, a la hora de realizar el registro de actividades (ver artículo 30 RGPD), podremos partir de los ficheros inscritos en el Registro General de Protección de Datos a la vista de la LOPD, así como de los procedimientos administrativos específicos que tenemos previstos o agrupados en nuestro gestor electrónico de expedientes para el cual tuvimos que hacer un inventario, y de los canales de entrada de datos personales (formularios, modelos de solicitud, bases reguladoras...). Respecto a esto último, además, nos sirve para actualizar dichos canales a las vicisitudes del RGPD. Todo ello nos da

bastante información de utilidad para conseguir realizar la tarea del análisis del tratamiento, y lo bueno es que sin darnos cuenta, ya contábamos con ello.

Lo mismo ocurre a la hora de identificar la licitud del tratamiento (ver artículo 6 RGPD). Como administraciones públicas partimos con la ventaja de que nuestra actuación debe encuadrarse necesariamente dentro de un marco jurídico competencial que nos legitima a hacer lo que hacemos, de tal suerte que esa norma con rango de Ley que ampara nuestra actividad administrativa, será también la base jurídica para cada actividad de tratamiento. De no ser así, no sólo tendríamos un problema con respecto a la protección de datos, sino con la nulidad de nuestros actos por incompetencia material (artículo 47.1 b de la Ley 39/2015). Sin perjuicio, claro está, de que existan determinados tratamientos cuya licitud venga determinada por otras bases jurídicas, como por ejemplo el consentimiento.

Como vemos, el desgranamiento de la estrategia, una vez definida, trae a su vez una serie de dificultades en la realización de las tareas por parte del responsable del tratamiento para el cumplimiento de cada *ítem* de la hoja de ruta, cuya solución es más sencilla de lo que pudiera parecer, y se encuentra, en muchos casos, en la propia organización.

4. CONCIENCIACIÓN Y RESISTENCIA DE LOS EMPLEADOS PÚBLICOS

La falta de concienciación y la resistencia de los empleados públicos son los principales ENEMIGOS de la correcta aplicación del RGPD. Aunque son conceptos diferentes, tienen el mismo resultado nocivo a la hora de poner en marcha cualquier proyecto. Es importante trabajar sobre ellos.

- La **RESISTENCIA AL CAMBIO** es un obstáculo para el progreso de las organizaciones. A nivel individual, forma parte del ADN de todos los trabajadores, más si cabe de los del sector público. No deja de ser un mecanismo de defensa de cara a lo desconocido, a lo que creemos que nos puede causar algún perjuicio –o simplemente no nos reporta ningún beneficio ni motivación– o porque nos suponga salir de nuestra zona de confort. La principal representación de la resistencia al cambio con respecto al RGPD, por parte del nivel institucional, es la demora en la implantación y en la adopción de medidas

tendentes al cumplimiento, dejarlo estar hasta que ya no haya más remedio que ponerse a ello. En el caso de los empleados públicos, suele manifestarse mediante la actitud negativa en nuestras obligaciones laborales, no realizando ninguna de las tareas asignadas, y a través de expresiones tales como: *"¡Buah! No teníamos poco con lo nuestro, que ahora nos mandan esto"; "La tecnología no trae más que problemas"; "Esto lo tendrán que hacer los de informática"; "Con lo a gusto que estábamos con el papel"; "Pues siempre lo hemos hecho así, y nunca ha pasado nada"; "Esto es idea de la chica nueva ésta que va de sabelotodo"; "Pues yo voy a seguir haciéndolo igual" "Ahora no hay más que derechos"; "¡Qué complicado!"; "Esto no sirve para nada más que para darnos más trabajo"; "Más tareas con el mismo sueldo"*. En definitiva, **creencias limitantes** que frenan la aplicación del RGPD, y perpetúan el desarrollo de malos hábitos en el tratamiento de datos personales.

- Con respecto a la **CONCIENCIACIÓN,** a nivel institucional, un dato representativo: De todas las entidades certificadas conforme al Esquema Nacional de Seguridad (ENS), sólo 2 son entidades locales (Avilés y Alcobendas) frente a unas 75 privadas.

  En este sentido, cabe destacar la encuesta realizada en octubre de 2017 (con el RGPD ya aprobado) por la Comisión de Sociedad de la Información y Tecnologías de la FEMP a Ayuntamientos mayores de 20.000 habitantes, sobre la adaptación de las entidades locales al nuevo reglamento europeo de protección de datos, cuya participación fue bastante baja (4 Ayuntamientos en Castilla y León) (ver encuesta). Los resultados ponen de manifiesto lo mucho que queda por hacer en materia de concienciación. Si bien el 80% sabe de la existencia del RGPD, el porcentaje se reduce al 60% con respecto a los que conocen los cambios que implican frente a la LOPD, y ya si nos adentramos en las medidas con las que cuentan los Ayuntamientos encuestados con respecto a dicho Reglamento, la cifra no supera el 40%.

  Pero es que además somos nosotros, como usuarios, los que no conocemos cuales son nuestros derechos en materia de protección de datos y como debe ser esa protección por parte de la entidad que los trata. De todas las quejas que se tramitan en la Agencia de Protección de Datos, sólo un 7%-8% de las

reclamaciones se refieren al sector público, eso sí, de ese pequeño porcentaje la mitad son sobre la administración local, como la más cercana al ciudadano. Se echa de menos una reflexión a nivel personal de cómo está siendo el tratamiento de nuestros datos, lo cual a su vez incentivaría la concienciación de quienes los tratan.

¿Por qué esta falta de concienciación en los empleados públicos?

Creencia limitante: *"Esto de la protección de datos no es cosa nuestra..."*

Efectivamente, el problema es que la normativa de protección de datos, es algo transversal a la organización, afecta a todos, y lo que afecta a todos en la administración acaba por no ser de nadie. Hay otras normas que tienen nombre y apellidos, es decir, llevan consignadas tareas nominativamente al área encargado de su ejecución. En el caso de la aplicación del RGPD, las diferentes dependencias no se sienten en la obligación de tener que cumplir lo que en él se dice o, al menos, no de la misma manera con que desempeñan sus funciones en el ámbito propio de su actuación. No lo identifican como una tarea del catálogo de servicios que les corresponden. Por ejemplo, entre las múltiples tareas que tienen, Fomento, identifica como un cometido propio, y a ello dedicará sus esfuerzos, el programa de subvenciones para el alquiler; Salud, la reducción de la lista de espera o la gestión adecuada del sistema de cita previa; Servicios Sociales la resolución de solicitudes de Dependencia; pero ninguno de estos áreas, siente como propio de su ámbito de actuación la protección de los datos que, por otra parte, afecta a todos y cada uno de estos programas o servicios mencionados. El problema es que cada dependencia, y en consecuencia la organización, basará sus éxitos en función de los logros conseguidos en cada uno de sus programas específicos y no, además, en base al grado de satisfacción en el cumplimiento del RGPD para la consecución de aquellos. Salvo cuando hay una quiebra en la seguridad, entonces ahí sí que nos acordamos del RGPD, y del DPD.

La falta de concienciación y la resistencia al cambio implican el desconocimiento de las obligaciones que impone la normativa y la inconsciencia de la gravedad de sus consecuencias, lo que provoca una serie de conductas, **malas prácticas,** que chocan diariamente con el contenido del RGPD:

- Publicaciones con exceso de datos personales, innecesarios para la finalidad que se pretendía conseguir.
- Publicaciones de imágenes personales en web, sin base jurídica que lo legitime.
- Notificaciones íntegras de una resolución que contiene datos personales sensibles de otros interesados.
- Pedir información superflua o innecesaria para el procedimiento que se está tramitando.
- Contraseñas débiles o mal custodiadas (post-it a la vista con contraseñas apuntadas).
- Usuarios y contraseñas genéricas o compartidas.
- Usuarios y contraseñas individualizadas, pero cuyo acceso se produce por personas distintitas a sus titulares.
- Mesas llenas de papeles con datos personales a la vista.
- Papeles con datos personales sin destruir en papeleras.
- Archivadores sin llave o falta de espacio para archivar expedientes.
- Documentos olvidados en las impresoras.
- Envíos por e-mail sin encriptar el contenido de la información adjunta.
- Utilización de USBs personales o sin cifrar.
- Reenviar información del trabajo a cuentas propias (Hotmail, Gmail....)
- Usar mecanismos de intercambio con terceros no validados. Dropbox, Google Drive.
- Mala orientación en las pantallas de los equipos que permiten la visibilidad de la información que éstas proyectan.

O incluso conductas que van más allá de la protección de datos y afectan a la **ética profesional:**

- Comentar casos o experiencias profesionales con referencias identificativas a nuestros compañeros o allegados.
- Comentar en el trabajo y fuera de él, las causas de excedencias o bajas laborales de los propios compañeros.
- Dar por teléfono o por e-mail información personal, sin asegurarnos de que quien está al otro lado es el interesado.
- Contar información personal a un tercero sin el consentimiento del interesado.

SOLUCIÓN ⟹ Gestión del cambio.

Frente a la inconsciencia y la resistencia…:

- **Información:** Es vital que cuando se pretende iniciar un nuevo proyecto se informe a los que van a tener que ejecutarlo sobre el mismo: qué lo motiva *¿por qué?*, que utilidad y finalidad tiene *¿para qué?*, qué tareas o carga de trabajo implica *¿qué?*, las ventajas o, en este caso, mejor las consecuencias de no hacerlo *¿por qué no?*

  Con la información conseguiremos:

  - Evitar los rumores que alimentan las creencias limitantes.
  - Que los empleados pierdan el miedo a lo desconocido.
  - Que conozcan lo que les va a suponer.
  - Dar valor a su actuación y que se sientan parte del proyecto mediante su participación.
  - El enganche con los más sensibilizados y proactivos, lo cual a su vez nos ayudará con los empleados resistentes.

  La información tiene que transmitirse de manera inicial, clara y concisa. Para ello, es recomendable reservar la parte inicial de la estrategia u hoja de ruta de la que hablamos en el punto 3, para mantener una reunión con los principales agentes que intervendrán en el proyecto (jefes/as o responsables de sección o servicio, o persona de referencia de esa dependencia). Y fijar un **nexo permanente de comunicación** eficaz, con capacidad resolutiva para cuando no se sepa algo, y que acompañe a los responsables durante todo el proceso de adaptación. En Diputación de Segovia, esta labor de información y permanente comunicación se está llevando a cabo por la figura del DPD.

- **Sensibilización:** Si no estamos sensibilizados difícilmente cambiaremos nuestros hábitos. A su vez, la sensibilización está muy ligada a la información. Si no conocemos algo, difícilmente seremos conscientes de lo que supone no hacerlo. Por eso, dentro de la información he resaltado la parte de las consecuencias de no hacerlo *¿por qué no?* En este punto, hay que poner en valor:

- la importancia de un adecuado tratamiento de los datos, del mismo modo que cualquier tarea propia del catálogo de cada área o servicio,
- lo que implica tanto a nivel legal como ético no hacerlo. Resaltar la gravedad del incumplimiento y ponerlo nombre de infracción (ver artículo 36 Ley 40/2015),
- identificar a los propios empleados como usuarios y titulares de datos personales en sus relaciones con las administraciones y con cualquier entidad, que sientan los perjuicios en sus carnes,
- las ventajas para su propio trabajo el actuar conforme al RGPD.

Todo ello nos ayudará a crear una cultura *pro* RGPD en la organización, con la que sin demasiados conocimientos específicos, podamos utilizar medidas sencillas. Que al menos nos paremos a pensar lo que vamos a hacer y cómo lo vamos a hacer. Muchas veces, la mejor medida para la protección es el sentido común. Pensar, *"si yo fuera el usuario, ¿me gustaría que tratasen así mis datos personales?" "¿Puedo conseguir la finalidad pretendida con el menor tratamiento posible?".*

- **Formación:** Ésta es la parte del *¿cómo?* que no se ha dicho en el apartado de la información. Hay que formar, decir cómo hacerlo. Es un error dar por hecho que nos hemos leído la norma y que todos conocemos las obligaciones que se nos suponen. Es necesario que todos los empleados conozcamos **cómo actuar en el ámbito que nos atañe según nuestra demarcación funcional**, ya que no todas las medidas tendremos que aplicarlas todos, ni tampoco en la misma intensidad. Dependerá de nuestra tipología de trabajo.

  En la formación, me parece importantísima la parte de los **principios RGPD.** Aprendiendo bien los principios evitamos buena parte de las malas prácticas anteriormente citadas (ver artículo 5 RGPD):

  - Con la *minimización de datos* haremos una reflexión de cuáles son los datos exclusivamente necesarios, de manera que evitaremos recabar información superflua y abundante,

- e innecesaria, con lo que tendremos que recapacitar, a su vez, sobre la finalidad de dicha información, y que sólo para eso se utilice *(limitación de la finalidad),*
- de manera *confidencial,* que además es un principio ético de los empleados públicos (ver artículo 53 Texto Refundido EBEP), así como con responsabilidad en la conservación *(integridad)*
- y proporcionando al interesado información sobre la necesidad del tratamiento de sus datos para el interés público o el cumplimiento de una obligación legal, de lo que se va a hacer con ellos y de los derechos que le amparan *(transparencia y lealtad),*
- siendo capaces de demostrar que estamos cumpliendo *(responsabilidad proactiva).* ¡**OJO**, pero cumpliendo! El problema de este principio es el abuso de su literalidad. No tenemos que quedarnos sólo con las formas ni con la imagen del buen hacer. No se trata de adaptar las cláusulas de los formularios, ni de publicar en la sede electrónica las actividades de tratamiento, ni los derechos que les corresponden a los interesados, sino de hacer realmente lo que dice el RGPD.

- **Instrucciones** claras que refuercen todo lo anterior. Es necesario que esta gestión del cambio requiera del impulso *"coercitivo"* que asegure su cumplimiento en forma de Circular, Instrucción, Acuerdo de Órgano de Gobierno... que ponga nombre y plazo a las tareas, e implique el traslado de la responsabilidad a quien corresponde. Es aconsejable no empezar por este punto. Que sea la parte final de la concienciación pero por la que se empiece el proyecto, que de formalismo al cambio por parte de la autoridad o cargo público que competa.

  En estas instrucciones es importante que se aclare el papel de cada uno. Que se diferencia el rol del DPD, con respecto al del responsable y encargado del tratamiento. **El DPD no es que el que tiene que aplicar el RGPD** sino informar, asesorar y realizar el seguimiento. **Al que le corresponde este cometido es al responsable y al encargado (según los casos), que será la organización**, si bien materialmente deberán acometerse por los diferentes áreas

o servicios (por quienes lo forman), como el resto de competencias de la administración.

Con todo ello, es muy probable que **corrijamos parte de nuestras malas prácticas:**

- Publicación de resoluciones con datos disociados. (Ej.: últimas cifras del DNI).
- Notificaciones de actos sólo en la parte que atañe a cada interesado.
- Publicación de una notificación por comparecencia sin necesidad de publicar todo el contenido de la publicación, (ver artículo 46 Ley 39/2015).
- Búsqueda constante de la relación base jurídica – tratamiento.
- Revisar los procedimientos administrativos con respecto a la necesidad de acceder a datos personales: ¿en qué medida es necesario el qué?
- Reducir la publicación masiva de imágenes personales en web y, en todo caso, buscar la base jurídica que lo legitime.
- Protocolos que limiten la accesibilidad por diferentes profesionales a datos personales. (Ej.: Remisión de informes a otros organismos a través de un registro auxiliar).
- Gestión de permisos, bajas y excedencia por un único profesional de referencia de RR.HH.
- Establecimiento de contraseñas y claves seguras.
- Mandar documentación adjunta encriptada.
- Restructuración de la oficina (Ej.: cambio de orientación de pantallas de ordenadores, mamparas o cristales tintados en salas de espera y de atención, insonorización de departamentos de atención, evitar papeles con datos a la vista, archivadores con llave, destructoras de papel nivel P4).
- Pedir referencias identificativas cuando hablemos por teléfono con terceras personas para comprobar que estamos tratando directamente con el interesado.

5. OBLIGACIÓN DEL SECTOR PÚBLICO VS NECESIDAD DEL SECTOR PRIVADO.

Otro **PROBLEMA** clave, a mi parecer, es que en **las administraciones públicas hacemos las cosas porque nos obliga una norma**. No tenemos la *"necesidad"* de cambiar nada para mejorar nuestra confianza en el usuario o mejorar nuestros servicios, o al menos ello no nos va generar un mayor rendimiento económico. Las

administraciones tenemos el monopolio de los servicios públicos, y de ello nos valemos ¿Habríamos publicado información en nuestros portales web sin la Ley de Transparencia? ¿Tendríamos registros electrónicos sin la Ley 39/2015? ¿Protegeríamos debidamente los datos personales sin el RGPD? Sin embargo, en las empresas las cosas se hacen por necesidad, de ello depende su viabilidad económica. Por poner un ejemplo, comparemos la usabilidad o amigabilidad en la compra de productos *on line*, con la de la tramitación de un expediente electrónico ante una administración pública ¿dónde es más sencillo?

Al hilo de esto vemos, además, que las empresas pagan las consecuencias de su incumplimiento, más allá de su perjuicio comercial. El RGPD, establece un régimen sancionador económico para ellas, NO así para las administraciones públicas. Aunque aún falta por ver cómo quedará en el Proyecto de Ley, parece que **no se va a prever un sistema de multas para las administraciones incumplidoras**. Lo que no tiene consecuencias, no es prioritario, por mucho que esté el principio de legalidad en la actuación administrativa y, en consecuencia, pasa a la cola de los fuegos a apagar.

SOLUCIÓN ¿Seguro que no tiene consecuencias económicas?

Quizá las administraciones no estemos sujetas a sanciones económicas en el RGPD, pero ello no significa que estemos exentas de **responsabilidad,** también **patrimonial**. La Ley 40/2015, prevé el derecho de los particulares a ser indemnizados de toda lesión en sus derechos por parte de las administraciones públicas (ver artículo 32 Ley 40/2015). Por lo que nada impide que puedan reconocerse los perjuicios por un inadecuado tratamiento de datos personales, a través del procedimiento de responsabilidad patrimonial de las administraciones públicas.

Es más, es que dicha responsabilidad exigida a la administración, como organización, puede repercutirse a sus autoridades y personal. Por lo que, a título individual, tampoco estamos exentos los **empleados** de incurrir en **responsabilidades** por "*dolo, o culpa o negligencia graves*" (ver artículo 36 Ley 40/2015)

Recordemos, también, los **principios éticos de los empleados públicos** a los que hacía referencia anteriormente. (ver artículo 53 Texto Refundido EBEP), que obliga al debido secreto profesional y confidencialidad.

O el derecho a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas (ver artículo 13 h) de la Ley 39/2015)

No obstante, sería conveniente pensar en la necesidad de hacer las cosas sin que tenga que haber una norma que nos obligue a ello. Hacerlo por obligación nos acaba llevando a pasar del cumplimiento al cumpli-MIENTO, es decir, en aparentar que cumplimos cuando en realidad no lo hacemos. Y aunque el grado de consecución en la adaptación a las necesidades de los ciudadanos no dependa de nuestra subsistencia económica, porque está claro que no vamos a quebrar, la falta de innovación nos ancla, y es un claro perjuicio para el interés general.

6. COMPLICIDAD DEL SECTOR PRIVADO.

PROBLEMA

De nada nos sirve cumplir nosotros, si no cumplen las entidades con las que trabajamos. El sector privado, entendido éste como el conjunto de las empresas o de las entidades con las que nos relacionamos en virtud de contratos públicos, convenios o cualquier otro instrumento jurídico, es clave para la aplicación del RGPD. Si sus herramientas de trabajo no tienen las funcionalidades que exige el RGPD, no cumplimos, aunque las nuestras sí que estén adaptadas.

SOLUCIÓN

Formalizar con las entidades un **contrato de encargado de tratamiento** con datos personales o cumplimentar e incluir en los convenios el **deber de diligencia**.

También ayudaría mucho el hecho de que se impusiese de algún modo en los Pliegos de contratación que las **empresas estén certificadas en el Esquema Nacional de**

Seguridad (ENS). Así, además, creamos un ecosistema de empresas cumplidoras, lo cual a su vez repercutirá en beneficio del resto de administraciones que se relacionen en un futuro con esas empresas, porque ya estarán certificadas.

Empresas certificadas en el ENS: https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/empresas-certificadas

7. ¿QUÉ NORMA CUMPLIR?

Nos encontramos en un momento de constante producción normativa que, además de dificultar el cumplimiento de las obligaciones que trae consigo por falta de medios en algunas administraciones, provoca cierta inseguridad jurídica al modificar constantemente el escaparate normativo.

Algunas de esas normas suponen la **confrontación de los derechos** que bajo su literatura amparan. Por un lado tenemos leyes cuya finalidad es que todos se sepa, y por el otro, otras que limitan esa publicidad ¿A qué derecho atenernos?

PROBLEMA:

Publicidad e Información VS Confidencialidad e Intimidad

Ley de Transparencia
Ley Gª de Subvenciones
Ley Gª Tributaria
TREBEP
Ley 39/2015
....

RGPD

La **SOLUCIÓN**, a mi parecer, pasa por hacer una **interpretación integradora y conciliable** de ambos bloques. Estar a cada caso concreto y **ponderar los bienes**

jurídicos objeto de protección, orientando nuestra decisión a la finalidad perseguida por cada norma en conflicto.

El propio ordenamiento funciona como un sistema de contrapesos en el que ninguna norma tiene que verse de manera absoluta, como una finalidad en sí misma. Son preceptos instrumentales y su aplicación debe orientarse al fin para el cual fueron concebidos.

Es importante no perder de vista la razón de ser de los mandatos en cuestión. **¿Cuál es la finalidad?** Con el derecho a la información y la publicidad que amparan estas leyes lo que se busca es: evitar la indefensión en los procedimientos administrativos por imposibilidad de notificación, no perjudicar a terceros interesados, limitar la discrecionalidad de los poderes públicos en su actuación, que se rinda cuentas por parte de los gobernantes, saber las diferentes actividades llevadas a cabo por las administraciones públicas, ver en qué se gasta el dinero público... En definitiva, una mayor participación del ciudadano en los asuntos públicos y en los procedimientos que se siguen en las diferentes administraciones. Pero es que esa finalidad quizá pueda lograrse con un **menor impacto en la esfera personal del afectado**, incluso en aquellos casos en los que el RGPD lo avala por tratarse del cumplimiento de una obligación legal o de una misión realizada en interés público. Y hasta pueda conseguirse esa finalidad a través de instrumentos que no permitan atribuir datos personales a un interesado a través de esa publicación (seudonimización). En definitiva **minimizar el tratamiento**

Por poner algún ejemplo:

- Es verdad que la Ley Gª de Subvenciones habla de la publicidad de las subvenciones (ver artículo 18 Ley Gª de Subvenciones, BDNS), pero ¿de todas y de la misma manera? Quizá la respuesta para muchos juristas sea la de que sí, pero yo tengo mis dudas pese a que incluso el RGPD puede que lo legitime. Para mí, no es lo mismo una convocatoria destinada a subvencionar los gastos derivados de la práctica deportiva de deportistas con una trayectoria reconocida, en cuyo caso la propia publicidad sirve de fiscalización con respecto al merecimiento de esa subvención y al logro los éxitos que sirvieron de base para la concesión, que una

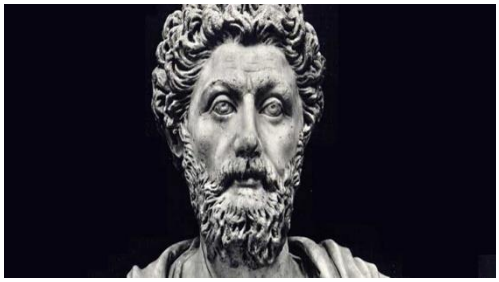
convocatoria para mujeres víctimas de violencia de género o ayudas destinadas a cubrir necesidades básicas de subsistencia en situaciones de urgencia social, en cuyo caso me parece excesiva la publicidad en proporción al derecho a la intimidad de las personas beneficiarias.

- La solicitud de acceso a la información por parte de una asociación sobre ayudas a la mujer embarazada en situación de exclusión social, deberá tramitarse en relación a la cuantía destinada a este concepto, en vez de a la identidad de las beneficiarias de las mismas. Si bien es cierto que la Ley de Transparencia es el máximo exponente de la publicidad activa, en su propio texto se limita el acceso a según qué información con datos personales e incluso se habla de la previa ponderación del interés público en la divulgación de la información y el derecho fundamental de la protección de datos personales (ver artículo 15.3 Ley 19/2013).

En definitiva, hacer un ejercicio de reflexión y motivación que nos lleve a tomar la decisión final en cada caso, y no dejarnos llevar por la literalidad aparente de la norma en cuestión

8. LIDERAZGO

Buena parte del éxito de cualquier proyecto depende de la capacidad de liderazgo que exista en la organización. Un liderazgo innovador, integrador, constructivo, capaz, valiente, comprometedor, permeable y latente.



Marco Aurelio

"Una fuerza más poderosa que el vapor, la electricidad y la energía atómica: la voluntad" (Albert Einstein)

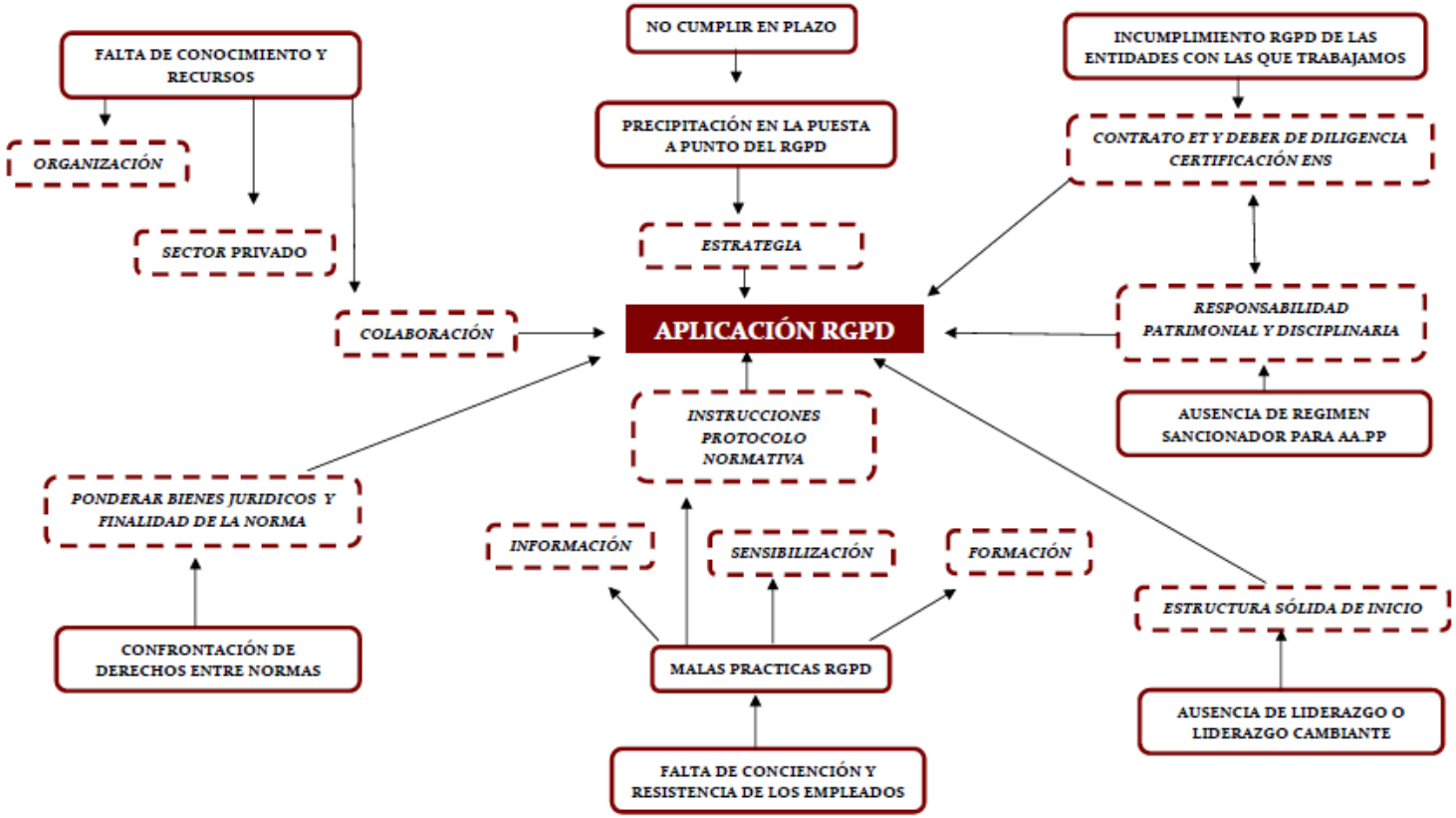
El **PROBLEMA** es que **falte ese liderazgo**, desde el punto de vista político y funcionarial. Que nadie ejerza de líder, o que el líder carezca de las virtudes precisas para ello; que nadie impulse y lidere el cambio ante las nuevas demandas sociales y normativas, de tal manera que todo siga igual lo que acabará por la involución de la organización. Otro **PROBLEMA** es que haya **liderazgo, pero cambiante**, como consecuencia de la movilidad funcionarial, o del agotamiento de la legislatura en el ámbito político.

La **SOLUCIÓN** pasa por un tándem directivo-político que asuman como propias las tareas tendentes al cambio, las impulsen, y creen a su vez una **sólida estructura** formada por puestos técnicos y administrativos capaces, impregnada por una actitud *pro* RGPD, que se mantenga para cuando vengan cambios. Que si se van las personas, no se vaya la cultura, el buen hacer, la filosofía, la esencia... De ahí la importancia en los inicios, de contar con un fuerte impulso político que avale el proyecto RGPD, que encuentre una buena alianza en el personal de la organización y que establezca los mecanismos e infraestructuras precisas ante cualquier amenaza cambiante: DPD colegiado, unidad o sección administrativa RGPD, comité de seguridad, etc.

Diputación de Segovia

ESQUEMA FINAL DE LOS PROBLEMAS Y SOLUCIONES

DPD



eclap
Escuela de Administración Pública de Castilla y León