CEU
Universidad
San Pablo

Comentarios a las "Directrices 4/2019 sobre el artículo 25 relativo a la Protección de Datos desde el Diseño y por Defecto"

Marta Palma Oliva

Comentarios a las "Directrices 4/2019 sobre el artículo 25 relativo a la Protección de Datos desde el Diseño y por Defecto"

Mi más sincero reconocimiento al Comité Europeo de Protección de Datos por su contribución a la delimitación y aplicación de la normativa de protección de datos personales en el entorno europeo y por contribuir a que seamos referente internacional en la materia. Estas Directrices son un claro ejemplo del compromiso asumido en el marco del artículo 70 del Reglamento General de Protección de Datos (RGPD en adelante) y es de agradecer el esfuerzo realizado por todos los expertos que contribuyen a dar forma a los cometidos de tan alta Institución.

Hoy me dirijo a ustedes tanto en calidad de estudiante del Máster de Protección de Datos de la Universidad San Pablo CEU de Madrid como de joven profesional inquieta y convencida de dedicar su carrera laboral al apasionante mundo del "dato". Apoyada en el deseo de poder serles de utilidad, tengan a bien considerar mi más humilde contribución a la protección de los datos personales a través de los comentarios que a continuación se exponen en relación con las "Directrices 4/2019 sobre el artículo 25 relativo a la Protección de Datos desde el Diseño y por Defecto".

Los comentarios se presentarán agrupados en dos grandes apartados. En primer lugar, se expondrán los relativos a la "FORMA" para, en segundo lugar, abordar los comentarios relacionados con el "FONDO" o contenido del documento.

FORMA

1) Forma estructural.

Debemos partir de la base de que las "Guidelines" deberían considerarse como unas directrices de utilidad en el desarrollo diario de cualquier actividad relacionada con la protección de datos personales. Ello quiere decir que, debería de poder ser una guía práctica para absolutamente todos los actores implicados: tanto para las Autoridades de Control, Legisladores, Responsables del tratamiento, Encargados, Delegados de protección de datos e incluso para los Profesionales del sector.

Cualquier maquillaje "burocrático", "protocolario" o "institucionalista" esta clase de documentos socava su cometido principal: la gestación del derecho fundamental a la protección de datos personales.

A nuestro juicio, estas Directrices se presentan un tanto generalistas o poco concretas. Para reflejar en la práctica un concepto tan ambiguo como es "la protección de datos desde el diseño y por defecto", las Instituciones relacionadas con la materia deberían asumir el compromiso moral de tomar la iniciativa para proporcionar esas "píldoras útiles de

información" sobre las que han de apoyarse los actores implicados para construir, en última instancia, dicho concepto indeterminado. Ello tiene incluso más relevancia en tanto que la protección de datos desde el diseño y por defecto se construye sobre la base del denominado "criterio del riesgo" y por tanto no existe un catálogo concreto de medidas técnicas y organizativas que conduzcan a un cumplimiento efectivo de los principios del tratamiento y a una garantía de los derechos y libertades de los interesados como impone el art.25 del RGPD.

Apoyándonos sobre esta base, animamos al Comité a que nos proporcione un mayor grado de detalle, mayor desarrollo y concreción, pues es la única forma para que el concepto que hoy estudiamos no quede huérfano de contenido. Para ello, invitamos al Comité a tener en cuanta los distintos ejemplos que, con la intención de poder serles útil en su labor, se exponen en el segundo bloque de este documento.

2) <u>Forma de transmisión del mensaje.</u>

Además de lo expuesto en relación con su forma generalista, existen, según nuestro criterio, otras razones que socavan la utilidad y practicidad del documento:

- <u>Repeticiones</u>: el contenido del resumen ejecutivo, así como el alcance (1) y las líneas introductorias de cada apartado del punto (2) es muy similar, lo que hacen un total de casi 6 páginas de contenido prácticamente idéntico.

- <u>Extensión</u> (27 páginas): teniendo en cuenta las repeticiones y adoptando iniciativas como el uso de formas más visuales para transmitir el mensaje (tablas, gráficos, colores…) con información concisa pero directa y útil, sería perfectamente factible reducir su número.

- <u>Análisis de cada Principio del tratamiento</u>: en efecto entendemos que, el cumplimiento de estos principios es una obligación directamente relacionada con la protección de datos desde el diseño y por defecto. Sin embargo, su objetivo real, o si se quiere, su reflejo práctico, es la adopción de las medidas técnicas y organizativas y de las garantías necesarias, es decir, los que vienen obligados por el art.25 deben de ACTUAR, por tanto ¿no sería más útil analizar otros extremos directamente relacionados con la configuración de estas medidas y garantías, en vez de ir uno por uno analizando el contenido de los principios del art.5º? Según nuestro criterio, el esfuerzo por analizar cada principio - punto (3)- lamentablemente, no aporta nada original y bien podría ubicarse perfectamente en otra "Guidelines" pero esta vez bajo la rúbrica: "Directrices sobre el art.5º RGPD relativo a los Principios del tratamiento". Por ser más rigurosos en el análisis, vamos a citar algunos ejemplos que, solo puntualmente, aportan algo novedoso: 1) Análisis del principio de equidad, 2) La invitación que hace el Comité a la revisión regular en relación con el principio de limitación del tratamiento o 3) Las limitaciones técnicas a la reutilización también en relación con este último. Estas son pequeñas excepciones que confirman que el punto (3) debería de sustituirse por otro tipo de contenido que propondremos a lo largo del presente documento.

Podemos concluir sobre este punto que, el "Principio de Transparencia", tan enérgicamente defendido, debería poder configurarse no solo en el contexto de la relación: Responsable-Interesado, sino también en el de la relación: Instituciones-Actores Implicados, predicando con el ejemplo. A la hora de elaborar esta serie de documentos, a nivel Institucional debería configurarse ese "Halo de Transparencia" en relación con sus obligaciones, transmitiendo el mensaje preciso y "de forma concisa, transparente, inteligible, de fácil acceso, con un lenguaje claro y sencillo", es decir, de manera práctica para los actores implicados.

3) <u>Forma de ilustración.</u>

Es de aplaudir la elección del Comité de presentar ejemplos prácticos ilustrativos, me parece una iniciativa muy útil y animo a continuar en esa línea. Sin embargo, y apoyándome en lo argumentado en el punto anterior, me parece que están excesivamente orientados a los principios de protección de datos en general.

Sería de agradecer que el Comité propusiese ejemplos relacionados con la actuación concreta de los actores implicados en la protección de datos desde el diseño y por defecto. Ejemplos como: un protocolo de actuación que preste especial atención al "momentum", medidas técnicas y organizativas concretas, garantías de los derechos y libertades… (opciones todas ellas que trataremos de analizar en el apartado siguiente). Estos "ejemplos" únicamente se observan a cuenta gotas en el apartado 6) de Conclusiones y Recomendaciones.

4) <u>Forma jurídica de la protección de datos desde el diseño y por defecto.</u>

Aunque no se trate propiamente de un comentario a ningún punto concreto de estas Directrices, no se nos ocurre lugar mejor para poder exponer una idea ya defendida por expertos en la materia, en ocasiones directamente y en otras, según nuestro criterio, implícitamente.

Lejos de ser una Obligación General, como reza el encabezado de la sección 1 del Capítulo IV del RGPD, la protección de datos desde el diseño y por defecto, no es sino el "Principio de Principios", básico y punto de partida de todos los demás, pues del análisis de su contenido se pone de manifiesto un cambio de paradigma en el ámbito del tratamiento de los datos personales.

La argumentación relacionada con esta propuesta disruptiva, se abordará con mayor detalle en el comentario siguiente (5), sin embargo se ha querido resaltar la propuesta en este apartado en tanto que, queremos recordar al Comité que si finalmente se configurase como principio, automáticamente se reforzaría el concepto, ya que el art.83 RGPD al establecer la graduación de sanciones impone las multas de mayor cuantía en caso de infracción de los principios básicos del tratamiento, y por el contrario, de acuerdo con su apartado 4, frente a las infracciones de las obligaciones recogidas en el art25, se impondrán las de menor cuantía.

La sociedad aún no está concienciada de este cambio de paradigma y es una lástima que haya que recurrir a medidas reactivas (imposición de sanciones) para poder garantizar las medidas preventivas (protección de datos desde el diseño y por defecto) pero parece la única vía para que se tengan en cuenta.

Alentamos al Comité a ser el fiel impulsor de esta idea pues valga recordar que el Derecho es una disciplina viva y en constante cambio, no sería descabellado considerar que tan alta Institución pueda rediseñar el concepto para su consideración como principio. Como es fácil de imaginar su ubicación en el RGPD sería difícil de modificar, sin embargo, las mutaciones legislativas son un elemento más del carácter vivo del ordenamiento jurídico.

FONDO

5) "Principio de principios"

Como avanzábamos en el apartado anterior, el principio a la protección de datos desde el diseño y por defecto podría ser considerado el "Principio de principios" por varios motivos:

- Implica toda actuación tendente a anticiparse y prevenir las posibles situaciones en las que exista una invasión de privacidad, se refiere al momento "PREVIO" a todo tratamiento, mucho antes de que entren en juego el resto de principios: "*en el momento de determinar los medios de tratamiento"* art.25.1 RGPD. Nunca podrán desplegar su efectividad real los principios de transparencia, minimización de datos, limitación del plazo de conservación… si no se ha aplicado previamente el principio de la privacidad desde el diseño.
- A la vez, se refiere a la configuración predeterminada de la privacidad, solo teniendo en cuenta el principio de la privacidad por defecto, recogido por el art.25.2 RGPD *"garantizar que por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines"*, podrán ser funcionales el resto de principios.
- "*En el momento del tratamiento*", como señala el art.25.1 tampoco debe perderse de vista este concepto. Este "DURANTE" la vida del tratamiento va más allá del propio alcance de los principios del art.5º, pues la aplicación los mismos parece orientada principalmente en prevenir los posibles riesgos derivados del tratamiento pero, ¿qué ocurre con tantos otros riesgos que no estaban previstos en el momento de diseñar el tratamiento, que ni siquiera tenían que ver en sus inicios con los datos personales? Parece que la aplicación de las medidas técnicas y organizativas, así como el establecimiento de las garantías apropiadas son las que van a hacer posible la configuración de la resiliencia en la privacidad. Por tanto, está el principio de protección de datos desde el diseño y por defecto, una vez más, por encima o en la base del resto de principios.
- Todos los actores, y no solo responsables y encargados como parece deducirse del capítulo del RGPD donde se ubica el precepto, están obligados a atender este principio. Las Directrices se repiten a lo largo de todo su articulado haciendo hincapié en este punto.

- Por último, intrínsecamente el art.25 no solo nos dice actúa ANTES, DURANTE Y DESPUÉS, sino que impone un nivel de estrés continuo en cuanto a la necesidad de DEMOSTRAR cada una de las actuaciones adoptadas en línea con sus cometidos, haciendo referencia a los ya famosos "*mecanismos de certificación*" de art.25.3. Por tanto, poco importa cumplir toda la extensa lista de principios del art.5º, pues hay que ser capaz de demostrarlo.

Por todo ello, lejos de la imposición de más obligaciones que no hacen sino sumar dificultades a la extensa lista de cargas a las que se someten los sujetos obligados por el RGPD, debería encuadrarse el "Principio de la protección de datos desde el diseño y por defecto" o "Principio de Privacy by design and default" como paradigma básico de la cultura la privacidad y seguridad en la sociedad de la información del s.XXI.

6) Objetivo principal de la protección de datos desde el diseño y por defecto

En el "Executive summary" las Directrices prometen ser una guía en relación con la obligación de la protección de datos desde el diseño y por defecto recogida en el art.25, sin embargo, a nuestro juicio, este enfoque se pierde de vista a lo largo del documento.

La idea de protección de datos o privacidad desde el diseño y por defecto existe desde hace más de 20 años y fue precisamente una de las impulsoras de esta "Privacy by design", Ann Cavoukian, la encargada de definir sus objetivos en la década de los 90. Para esta Comisionada de la Protección de Datos de Ontario, los objetivos sobre la materia en cuestión se centran en:

1º. Asegurar la privacidad y obtener el control personal de la propia información,

2º. Permitir obtener una ventaja competitiva sostenible a las organizaciones.

En nuestra opinión, relegar al olvido su preciado trabajo "7 Foundational Principles of Privacy by Design" sería un desperdicio, por ello invitamos a tomarlos como referencia para poder presentar opciones reales, con reflejo en la práctica. Según la autora, los siguientes principios son básicos para poder alcanzar el objetivo doble de la "Privacy by design":

1. Proactivo, no reactivo; preventivo, no correctivo: se trata de identificar todas las debilidades de los sistemas para neutralizar y minimizar los riesgos, y así evitar que se conviertan en daños.
    - ➔ En la práctica: identificar a priori los posibles riesgos a los derechos y libertades de los interesados y minimizarlos y todo ello hay que hacerlo desde cero, en el momento de utilizar cualquier sistema, proceso o infraestructura. Yendo más allá, podría incluso pensarse en el posible y lejano desarrollo natural del negocio o la aplicación, para poder anticiparse en la medida de lo posible (estaríamos siendo fieles al "estado de la técnica" en su máximo exponente). Este compromiso debe impulsarse desde los niveles superiores de la organización pero sin olvidar

que hay que construir una "gobernanza de la privacidad" que se traduce en implicar a todos los actores en el mismo nivel para poder desarrollar la cultura de la privacidad.

2. La privacidad como configuración predeterminada: tanto las TIC's como las concretas operaciones del tratamiento deben estar configuradas desde el inicio para proteger la privacidad.
    - ➔ En la práctica: aunque el interesado no adopte ninguna acción de configuración de su privacidad, que por defecto su privacidad ya esté configurada de la manera más garantista (cuidado con ser demasiado garantistas en el sentido que el interesado no sea capaz de revertir el proceso para desbloquear opciones de privacidad, recuérdese que tiene que poder disponer de sus propios datos). Deberán fijarse criterios de privacidad, accesos restringidos…

3. Privacidad incrustada en el diseño: la privacidad pasa a ser parte integral del sistema sin disminuir su funcionalidad (relacionado directamente con el siguiente principio).
    - ➔ En la práctica: Considerar la privacidad como un requisito imprescindible para todo el ciclo de vida de los sistemas, servicios y procesos de una compañía.

4. Funcionalidad total: "todos ganan". No se sacrifica privacidad por funcionalidad, ni al revés. Es esencial encontrar este equilibrio, perfectamente posible y que solo genera externalidades positivas.
    - ➔ En la práctica: identificar, evaluar y sopesar los distintos intereses implicados, los de la entidad en cuestión y de los interesados. Opciones como facilitar canales de cooperación y diálogo pueden ser interesantes.

5. "Seguridad de extremo-a-extremo" protección de todo el ciclo de vida: es imprescindible integrar la privacidad a lo largo de todas las etapas del tratamiento que necesariamente implican distintas operaciones desde la recogida, registro, clasificación, conservación, consulta, difusión… y adaptar la protección de la privacidad a cada una de ellas. Para ello es capital que las instituciones como el Comité se posicionen tajantemente sobre criterios como "plazos de conservación" para facilitar la grandiosa tarea de cumplir con la privacidad a los sujetos obligados.
    - ➔ En la práctica: el cifrado por defecto, la destrucción segura, plazos de conservación bien definidos por las autoridades…

6. Visibilidad y transparencia: una de las claves para garantizar la privacidad es poder demostrarla, verificando que el tratamiento es acorde a la información dada, para ello, la transparencia y accesibilidad se vuelve un pilar para demostrar esta proactividad.

- ➔ En la práctica: ello no tiene que ver exclusivamente, como parecen defender las Directrices en el análisis del principio de transparencia (punto 3), con cumplir con el principio de transparencia como diseño de política de protección de datos en relación con el tratamiento de datos personales, sino con ir más allá publicando informes de transparencia en cuanto al compromiso asumido por la organización en su conjunto respecto de la transparencia (Iniciativas que las grandes empresas proveedoras de servicios de internet ya han comprobado que se traducen en ventajas competitivas respecto de sus rivales. Google, Facebook o Amazon ya publican regularmente informes de transparencia).

7. Mantener un enfoque centrado en la privacidad de los usuarios: cualquier decisión o medida que se adopte en una organización debe prever la garantía de los derechos y libertades de los interesados-usuarios, sin perjuicio de buscar la consecución de los intereses legítimos de la compañía.
   - ➔ En la práctica: el usuario debe poder tener un papel activo en la gestión de sus datos personales y ello se consigue con la configuración de políticas de privacidad efectivas, garantía del ejercicio de derechos…

7) "Ingeniería de la Privacidad" - AEPD

Pero además de apoyarnos en todos estos principios para delimitar el objetivo de la protección de datos desde el diseño y por defecto, los sujetos implicados necesitan más recursos prácticos. Sobre esta base, invitamos al Comité a que se apoye en la guía de privacidad desde el diseño que ha publicado la Agencia Española de Protección de Datos (AEPD) https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf.

Este documento examina la denominada "Privacy Engineering" configurada como un proceso sistemático y dirigido por el enfoque del riesgo cuyo objetivo es traducir en términos prácticos y operativos los principios de la privacidad desde el diseño, que también se recogen en él.

8) Catálogo de medidas técnicas y organizativas.

Es cierto que el art.25 RGPD establece que el Responsable del tratamiento deberá tener en cuenta los diversos factores que puedan concurrir en una actividad de tratamiento, como puede ser la tecnología disponible, los costes de su aplicación y por supuesto la naturaleza, ámbito, contexto y fines del tratamiento, junto con los riesgos que potencialmente puedan suponer las operaciones del tratamiento para los derechos y libertades de las personas físicas.

Todo ello genera ya de por sí ambigüedad y ciertamente, frustración para los sujetos obligados. Por tanto, una institución como el Comité de Protección de Datos podría publicar una guía de medidas técnicas y organizativas que, aún no siendo consideradas en ningún caso "numerus clausus" si iluminen el camino a los actores. Una ocasión como la de publicar las

Directrices de la protección de datos desde el diseño y por defecto no puede desaprovecharse para acometer este esfuerzo.

9) Protocolo de actuación

Al tener el principio de privacidad desde el diseño y por defecto tan amplio impacto en el "timming" de la protección de datos, se propone también, recoger en estas Directrices un protocolo de actuación que examine las diferentes fases presentes en el ciclo de vida de todo tratamiento de datos. Sería interesante plantear este protocolo a modo de preguntas en relación con las distintas fases. A modo de ejemplo:

1- Planeamiento del tratamiento ¿realmente es necesario el tratamiento de estos datos personales?,
2- Recogida de datos ¿está recopilando únicamente los datos necesarios para alcanzar la finalidad concreta?,
3- Tratamiento ¿Dispone realmente de base jurídica habilitante para llevar a cabo el tratamiento de los datos personales?,
4- Conservación ¿ha analizado la legislación aplicable a la tipología de datos que pretende tratar y tomado como referencia los plazos genéricos que recoge?,
5- Accesibilidad ¿Dispone de fichas modelo para el efectivo ejercicio de los derechos que asisten a los interesados?
6- Destrucción ¿Dispone de un método seguro de eliminación de datos que imposibilite un acceso futuro a los datos personales?

Pero además no podemos olvidar otro punto clave que ha de figurar en el protocolo: la necesidad de demostrar su cumplimiento.

10) Demostrar su cumplimiento

El art.25.3 RGPD dispone que: "*podrá utilizarse un mecanismo de certificación como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo*". La atención que las Directrices otorgan a este apartado parece ser pobre teniendo en cuenta que se trata de un concepto polémico que está originando más de un quebradero de cabeza a los Estados Miembros.

El artículo deja abierta la posibilidad de utilizar esta clase de mecanismos por tanto, el Comité podría concretar las alternativas válidas que puedan tenerse en cuenta por las Autoridades de Control para poder demostrar el cumplimiento.

Podría por ejemplo optarse por un sistema de cumplimiento por niveles, o una referencia de cumplimiento por sectores de actividad o atendiendo a la sensibilidad de la información objeto del tratamiento… una vez más se ha dejado pasar la oportunidad de concretar algo tan importante como son los sellos de calidad o códigos de conducta.

CONCLUSIÓN

Para concluir, animamos una vez más, al Comité Europeo de Protección de Datos a repensar las Directrices 4/2019 sobre la protección de datos desde el diseño y por defecto y a poder considerar la idea de plantear este concepto como “Principio de principios” para dotarlo de la importancia que le merece.

En Madrid a 14 de enero de 2020.