Melba H. Santa Coloma Yabur

MÁSTER UNIVERSITARIO EN PROTECCIÓN DE DATOS,

TRANSPARENCIA Y ACCESO A LA INFORMACIÓN

Comentarios a las Directrices 04/2019 del Comité Europeo de Protección de Datos, sobre el artículo 25 RGPD. Protección de Datos desde el Diseño y por Defecto.

Nota: En negro mis comentarios. En azul, el texto citado.

- Resumen ejecutivo

- *Para garantizar una adecuada protección de los datos, el responsable del tratamiento debe revisar periódicamente la efectividad de las medidas elegidas.*

Sería recomendable que se estableciera el periodo de tiempo, o al menos los plazos máximos para realizar dichas revisiones. De lo contrario, parece difícil demostrar si el responsable ha obrado de manera negligente o no, ya que queda sujeto a su propia interpretación qué se entendería por una revisión "periódica".

- *El concepto de "estado de la técnica" requiere que los responsables del tratamiento se mantengan actualizados sobre el progreso tecnológico, para asegurar la implementación continua y efectiva de los principios de protección de datos.*

El 99% de los responsables de tratamiento de la Unión Europea son PYMEs, según la ficha técnica sobre la Unión, https://www.europarl.europa.eu/factsheets/es/home. Resultaría una misión complicada para muchas de estas pequeñas y medianas empresas mantenerse al día sobre el estado de la técnica, por carencia de medios económicos y falta de capacidades técnicas. Por otra parte, ésta tarea debería encomendarse no solo a los responsables del tratamiento, sino principalmente a los responsables de fabricar y desarrollar los sistemas de tratamientos de datos. Ellos deberían tener la obligación de mantener una formación continua de sus clientes (los responsables del tratamiento) e incluso de aquellos que no lo son, sobre las

actualizaciones y novedades técnicas de los sistemas o dispositivos que lanzan y sostienen en el mercado. Las autoridades de control y organismos europeos también pueden colaborar en esta labor, publicando artículos, enlaces, tutoriales y guías que ayuden a cualquier ciudadano, aunque no tenga una formación técnica, a mantenerse al día sobre dichos avances. Esto podría incluirse en los derechos digitales.

- *Esto requiere que los responsables implementen medidas técnicas y organizativas apropiadas y salvaguardas necesarias, diseñadas para implementar principios de protección de datos de manera efectiva y para proteger los derechos y libertades de los interesados. Los controladores deben poder demostrar la efectividad de las medidas implementadas….*
- *… Otros elementos que los responsables del tratamiento deben tener en cuenta son la naturaleza, el alcance, el propósito del tratamiento y el riesgo que comporta.*
- *"Naturaleza, alcance, contexto y propósito del tratamiento"*
  25) Los responsables deben tener en cuenta factores como la naturaleza, el alcance, el contexto y el propósito del tratamiento a la hora de determinar las medidas técnicas y organizativas apropiadas implementar efectivamente los principios en el tratamiento.

Me pregunto ¿cómo pueden sostenerse los principios de protección de datos en el uso del Big Data, cuyo sentido resulta por naturaleza contrario a estos principios? La razón de ser del Big Data es captar la mayor cantidad de datos posible. Al responsable del tratamiento (o responsables) en muchas ocasiones les resulta imposible conocer de antemano la naturaleza, alcance, el contexto o propósito del tratamiento, como ocurre en el caso de la minería de datos. Por tanto, resulta imposible, por ejemplo, cumplir con la obligación de informar a los interesados. También pierde el interesado el poder de control sobre sus datos, ya que estos se diluyen a través de las distintas etapas del procesamiento del Big Data. En cuanto a la anonimización y la interrogante de si los datos que se tratan en Big Data son datos personales o no, la Autoridad de Control española, en su informe "Orientaciones y garantías en los procedimientos de anonimización de datos personales" https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf, concluye que "*existe una proporcionalidad manifiesta en lo que respecta a la capacidad tecnológica de anonimizar y la posibilidad de la reidentificación de las personas cuyos datos han sido anonimizados, es decir, la misma capacidad de la tecnología para anonimizar datos personales puede ser utilizada para la reidentificación de las personas… No es posible considerar que los procesos de anonimización garanticen al 100% la no reidentificación de las personas, por lo que será necesario sustentar la fortaleza de la anonimización en medidas de evaluación de impacto (EIPD), organizativas, de*

seguridad de la información, tecnológicas y, en definitiva, cualquier medida que sirva tanto para atenuar los riesgos de reidentificación de las personas como para paliar las consecuencias de que éstos se materialicen."

- *Las directrices contienen, además, una guía práctica sobre cómo implementar de manera efectiva los principios de protección de datos del artículo 5 RGPD, señalando elementos clave de diseño y por defecto y ejemplos prácticos a modo ilustrativo.*

Es de agradecer que se ofrezcan ejemplos prácticos. Sin lugar a dudas serán de utilidad para muchos responsables del tratamiento. Considerada la protección de datos un derecho fundamental, es importante que tengamos muy clara la normativa y seamos concisos y tajantes en su aplicación. Sin embargo se echan en falta orientaciones técnicas dirigidas a los profesionales que fabrican y desarrollan los medios de procesamiento de datos, y un organismo de control directo y efectivo sobre la aplicación de estas orientaciones técnicas.

- *Para finalizar, el CEPD ofrece recomendaciones sobre cómo los responsables del tratamiento, procesadores y proveedores de tecnología pueden cooperar para lograr una protección de datos desde el diseño y por defecto y cómo esta puede usarse como ventaja competitiva.*

Convertir el DPbDD en una ventaja competitiva es una manera muy inteligente de fomentar la implementación efectiva de los principios de protección de datos desde el diseño y por defecto. Es ahí a donde debemos llegar. Sin lugar a dudas. Pero hasta alcanzar ese objetivo es necesario concienciar a todos los ciudadanos acerca de la importancia de sus datos, de la importancia de que los protejan. Deben realizarse campañas de concienciación tanto en colegios como en otros medios de información, dirigidos no solo a menores sino también a adultos. Los ciudadanos ya no queremos pagar por los productos que adquirimos en internet y las grandes compañías se aprovechan de ello. Pero la obligación de formar y concienciar acerca de la importancia de proteger los datos personales no debería recaer solamente en la Unión Europea o en los Estados miembros. También los responsables deberían estar obligados a formar a los usuarios (interesados) acerca de la importancia que tienen sus datos para las empresas y lo vulnerables que podemos ser los ciudadanos si nuestros datos no son tratados correctamente.

Además se debería regular una nueva obligación para los responsables del tratamiento: la obligación de informar sobre cuál es el precio real de los productos que ofrecen gratis o a costes mínimos. De modo que los consumidores sepamos el precio real de aquello que adquirimos “gratis”.

- 1) Alcance

- *1) …Otros actores, como los procesadores y proveedores de tecnología que no se mencionan directamente en el artículo 25, también pueden encontrar útiles estas directrices para la creación de productos y servicios acorde con el RGPD, que permitan a los responsables cumplir con sus obligaciones.*

Además de las directrices, que sin dudas serán de gran ayuda para los fabricantes, desarrolladores y proveedores de tecnología, debería crearse un código ético de obligatorio cumplimiento para los mismos.

- *…El considerando 78 del RGPD señala que la protección de datos desde el diseño y por defecto debe tenerse en cuenta en el marco de las licitaciones públicas. A pesar de que todos los responsables tienen el deber de integrar la DPbDD en sus actividades de tratamiento, esta disposición fomenta la adopción de principios que las administraciones públicas deben poner en práctica para liderar con el ejemplo.*

Me parece muy buena esta iniciativa que las administraciones públicas no sólo apliquen en primera línea los principios de transparencia y protección de datos, sino que exijan que sus proveedores también cumplan. Deberían extender esta obligación no sólo a los productos que son contratados por la administración, sino a todos los productos que fabriquen o comercialicen los proveedores de la administración. Que todos sus proveedores cumplan con los principios de protección de datos desde el diseño y por defecto y a la vez exijan el cumplimiento de sus proveedores y clientes. Deberían crearse medios de verificación efectiva de este cumplimiento.

- *4) Las Directrices también abordan en el capítulo 4 la posibilidad de establecer un mecanismo de certificación para demostrar el cumplimiento de acuerdo con el artículo 25, y en el capítulo 5 aborda la forma en que este artículo puede ser aplicado por las autoridades de supervisión.*

Esta es una iniciativa muy positiva y necesaria. Sin embargo, espero que el coste no resulte demasiado elevado para los responsables del tratamiento, que como se dijo anteriormente, son en su mayoría son pequeñas y medianas empresas. Estas certificaciones deberían ser obligatorias en el caso de fabricantes, desarrolladores y grandes compañías, cuyo activo depende fundamentalmente de los datos. No para pequeñas empresas.

- Análisis del artículo 25

- *9) Una medida técnica u organizativa puede ser cualquier cosa, desde el uso de soluciones técnicas avanzadas hasta la formación básica del personal, por ejemplo, sobre cómo manejar los datos del cliente.*

La formación básica del personal es una medida idónea, económica y razonable. La formación es fundamental. Los responsables del tratamiento deberían formar efectivamente a sus empleados porque ellos son la principal brecha en una empresa. El problema es que esta formación a veces resulta costosa para las pequeñas y medianas empresas. Podrían crearse programas de incentivo para propiciar estas formaciones, teniendo en cuenta que las formaciones se realicen siempre por profesionales que puedan acreditar su formación en protección de datos.

- *10) La posibilidad de que los interesados intervengan en el tratamiento, proporcionándoles información automática y repetida sobre qué datos personales se almacenan, o tener un recordatorio de almacenamiento en un repositorio de datos pueden ser ejemplos de medidas de protección necesarias.*

Como se dijo anteriormente, el tratamiento de datos basado en Big Data, por sus características resulta contrario a los principios de DPbDD. En estos procesos no se puede informar sobre qué datos se almacena ni qué tipo de tratamientos de realizan porque no es posible saberlo ni para el propio responsable. También se hace difícil la participación activa del interesado porque se pierde el control de los datos.

- *13) A la hora de implementar las medidas técnicas y organizativas apropiadas, deben diseñarse las medidas y salvaguardas respecto a la implantación efectiva de cada uno de los principios, derechos y libertades mencionados anteriormente.*

Se echan en falta propuestas reales, modelos, ejemplos y medidas técnicas de obligatorio cumplimiento. También sería positiva la creación de una entidad que se ocupe de supervisar el cumplimiento efectivo de los requerimientos por parte de fabricantes, desarrolladores, proveedores de servicios de la sociedad de la información y responsables.

“Coste de implementación”

- *24)…El responsable debe evaluar el coste de implantar efectivamente todos los principios. La incapacidad para asumir este coste no justifica el incumplimiento del GRPD. Al mismo tiempo, la implantación efectiva de los principios no debe conllevar necesariamente a un aumento de los costes. Un mayor gasto en tecnología no conduce necesariamente a una implantación más efectiva de los principios.*

En España se aprecia una falta de concienciación por parte de la mayoría de responsables de tratamiento, que aún consideran la protección de datos (y sus costes) un capricho del legislador. Muy pocos responsables tienen en cuenta los costes de implantación de los principios de protección de datos desde el diseño. Los profesionales de la protección de datos en España encontramos muchas dificultades para mantener los precios de nuestros servicios en el mercado, porque el cliente no está concienciado de que necesita una orientación profesional avalada para garantizar los derechos y libertades de los interesados. Esto facilita el intrusismo por parte de empresas que, sin tener la preparación adecuada, ofrecen el servicio de protección de datos a precios irrisorios, incluso a coste cero, aprovechando para vender otros servicios. Esto se convierte en una espiral: el responsable no se cree que es importante tener una protección de datos adecuada - el intruso se aprovecha y ofrece servicios a costes irrisorios -los principios de protección de datos no se implantan correctamente -mientras el responsable cree que cumple porque una empresa le ha hecho la protección de datos.. y así sucesivamente, va creciendo la espiral. A nadie se le ocurriría dejar sus finanzas en manos de alguien que no entiende de números. Del mismo modo es importante que los responsables de tratamiento tomen conciencia de la importancia de elegir **profesionales capacitados**. En este sentido, y después de haber lanzado varias quejas y denuncias que no han sido resueltas, apelo al Comité Europeo de Protección de

Datos en apoyo a los profesionales españoles del sector. Para garantizar una implantación efectiva de los principios de protección de datos, los profesionales necesitamos protección ante el intrusismo, y esto solo se consigue a través de la concienciación de los interesados sobre la importancia de proteger los datos e implantar correctamente los principios de DPbDD. Se me ocurren diferentes vías, como la creación de mecanismos de certificación que sean obligatorios a la hora de prestar un servicio de protección de datos, la creación de colegios oficiales, la creación de una comisión que nos proteja ante estas prácticas, un canal de denuncias con respuesta efectiva y contundente,etc.

- *2.1.4 Aspecto del tiempo*

  En el momento de la determinación de los medios de tratamiento

- *32) La protección de datos desde el diseño debe implantarse " en el momento de la determinación de los medios utilizados para el tratamiento ".*

A las grandes compañías, que sirven de ejemplo al resto, no parece interesarles la privacidad desde el diseño. Tenemos ejemplos como Google Street View, donde se podía acceder a los datos de muchas redes wifi que se encontraban en los lugares recorridos o Facebook Apps que cedía la información de los usuarios que se instalaban las apps, el escándalo de Cambridge Analytica, entre otros. Estos incidentes, entre otros que ocurren cada día, se habrían podido evitar con una correcta política de privacidad desde el diseño. A algunas grandes compañías, cuyo principal activo son los datos, parece resultarles más lucrativo implantar la privacidad “a posteriori”, y no desde el diseño.

- Transparencia

- *El diseño clave y los elementos predeterminados pueden incluir un multicanal: la información debe proporcionarse en diferentes canales y medios, más allá del textual, para aumentar la probabilidad de que la información llegue efectivamente al interesado.*

La difusión a través de canales múltiples me parece una medida muy interesante para conseguir que la información llegue realmente a los interesados.
Finalmente quiero agradecer al CEPD por su labor y animarle a que siga trabajando por la consolidación y defensa este derecho fundamental y humano.