PROTECCIÓN DE DATOS VS. PREVENCIÓN DE BLANQUEO DE CAPITALES

Un análisis desde el ordenamiento legal español

Víctor Altimira Ávalos*

Este artículo pretende reflejar las relaciones entre dos normativas, que en principio no tienen nada en común, pero que están llamadas a entenderse.

Y tienen que entenderse, bien porque así lo decide el legislador, bien porque es esencial para el buen funcionamiento del negocio del sujeto obligado[1].

Ni la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) ni su Reglamento desarrollador (Real Decreto 1720/2007, de 21 de diciembre, en adelante RLOPD) hacen mención alguna, ni de forma directa ni indirecta, a los datos que provienen de la prevención del blanqueo de capitales ni de la financiación del terrorismo.

Es en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (en adelante LPBCYFT), donde encontramos las referencias a la normativa de protección de datos de carácter personal.

Concretamente los artículos 15, 32 y 33 de esta norma obligan a:

- **Crear un fichero o ficheros** para las finalidades establecidas en la normativa de prevención de blanqueo de capitales y la financiación del terrorismo e inscribirlo en la Agencia Española de Protección de Datos. Recordemos que según el artículo 5.1k) del RLOPD por fichero entendemos *"todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso."*
- La creación de un único fichero o de varios será discrecional, a tenor de si el sujeto obligado desea dividir su contenido entre **datos de personas con responsabilidad pública y resto de personas, o no.**

Especial para la revista Pensamiento Penal.

*Vicepresidente del Instituto de Expertos en Prevención de Blanqueo de Capitales y Financiación del Terrorismo (INBLAC). Vocal Responsable de Privacidad de la Sección de Derecho de las Tecnologías de la Información y de la Comunicación del Ilustre Colegio de Abogados de Barcelona (2010 - 2013). Abogado de Logic Data Consuting, S.L.

[1]El listado completo de los sujetos obligados se encuentra en el art. 2 de la LPBCYFT.

- El **fichero o ficheros** creados deberán cumplir con las **medidas de seguridad de nivel alto,** previstas en la normativa de protección de datos de carácter personal. Es decir, que la LPCYFT amplía el artículo 81.3 del RLOPD y estos ficheros se equiparan a los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, así como los que contienen o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas, y aquellos que contengan datos derivados de actos de violencia de género.
- **El sujeto obligado no tendrá la obligación de informar al cliente o posible cliente** conforme a la normativa de protección de datos para incluirle en dichos ficheros. Por tanto, en esta ocasión aplicamos lo dispuesto en el artículo 6.1 de la LOPD que dispone que *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa".* Está claro que la LPBCYFT ha dispuesto otra cosa.
- El sujeto obligado podrá recabar la información disponible sobre personas con responsabilidad pública sin contar con el consentimiento de éstas, aunque esta información **no se encuentre disponible en fuentes accesibles al público**. En esta ocasión, el sujeto obligado para cumplir con la famosa obligación del KYC (KnowYourCustomer) puede acudir a cualquier fuente de información aunque no sean públicas[2].

[2]Fuentes accesibles al público: El artículo 3 letra j) de la LOPD define así la fuentes accesibles al público: "Aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación." El artículo 7 del RLOPD extiende y aclara: 1. A efectos del artículo 3, párrafo j) de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público:

a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.
b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.
c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse colegiado, fecha de incorporación y situación de ejercicio profesional.

d) Los diarios y boletines oficiales.

e) Los medios de comunicación social.

2. En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona,

- **Tampoco tendrá la obligación de tener el consentimiento del cliente o cliente potencialpara ceder sus datos personales** a la autoridad competente en materia de lucha contra el blanqueo de capitales o financiación del terrorismo. En esta ocasión debemos acudir a lo dispuesto en el artículo 11.1 de la LOPD: *"Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado",* si bien el consentimiento no será necesario, conforme al artículo 11.2 a) *"en caso de que la cesión se encuentre amparada en una norma con rango de Ley".* Es por ello que no se requiere el consentimiento en estos casos[3].

- **Los sujetos obligados podrán intercambiar información entre otros sujetos obligados y ficheros centralizados de prevención del fraude, relativa a las operaciones referidas en los artículos 18 y 19 de la LPBCYFT**, *"….. cuando de las características u operativa del supuesto concreto se desprenda la posibilidad de que, una vez rechazada, pueda intentarse ante otros sujetos obligados el desarrollo de una operativa total o parcialmente similar a aquélla".* De la lectura de los dos artículos citados se desprenden dos consecuencias en relación al contenido de las operaciones respecto de las cuales se podrá producir el intercambio de la información:

  1) Debe tratarse, en todo caso, de operaciones que hayan sido objeto de comunicación al SEPBLAC, Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. Lo que en Argentina viene siendo la UIF.

  2) La comunicación únicamente podrá referirse, de entre las operaciones descritas, a aquéllas respecto de las que pueda ser previsible el intento de comisión reiterada ante otro sujeto obligado, coincidiendo la operativa llevada a cabo por el supuesto infractor en ambos casos.

  Huelga comentar, que en esta caso también prevalece la excepción del consentimiento del afectado comentado en el punto anterior.

- **En cuanto al ejercicio de los derechos de acceso, rectificación, cancelación y oposición**,que puedan ejercitar las personas incluidas en estos ficheros, los sujetos obligados no deberán aplicar la LOPD y se limitarán a poner de manifiesto lo dispuesto en el artículo 32 de la LPCYFT. También se regula este aspecto en el artículo 33.5 del mismo cuerpo legal. Los conocidos derechos ARCO, se regulan tanto en la LOPD (artículos 15 a 17) como en el RLOPD (a los que se les dedica todo el Título III). No obstante, el afectado siempre podrá, y

---

no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.

[3]para más información sobre las cesiones de datos en materia de prevención del blanqueo de capitales y financiación del terrorismo ver Informe Jurídico 0517/2010 de la Agencia Española de Protección de Datos.

así se le tendrá que comunicar en la denegación del derecho ARCO que corresponda, ejercitar el derecho de tutela ante la Agencia Española de Protección de Datos (artículo 18 LOPD).

- **Únicamente podrán utilizar los datos contenidos en dichos ficheros para el cumplimiento de las medidas reforzadas** de diligencia debida previstas en la LPBCYFT. Este punto debemos ampliarlo con lo dispuesto en el artículo 33 de la misma Ley sobre el intercambio de información entre sujetos obligados y ficheros centralizados de prevención del fraude. Concretamente cuando se refiere en su apartado cuarto a que *"el acceso a los datos a los que se refiere este precepto deberá quedar limitado a los órganos de control interno previstos en el artículo 26, con inclusión de las unidades técnicas que constituyan los sujetos obligados."* Para analizar este punto, debemos tener en consideración la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011 cuando regula el efecto directo del artículo 7 f) de la Directiva 95/46/CE, según el cual *"Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva".*

  Dicha Sentencia, en su apartado 38, indica que el precitado artículo 7 f) de la Directiva *"establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado"* y, en relación con la citada ponderación, el apartado 40 recuerda que la misma *"dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea confieren al interesado"*.

  Por todo ello, para valorar si existe o no un interés legítimo por parte del responsable del fichero o del tratamiento en estos casos, debemos tener en consideración lo manifestado en el Informe Jurídico 0404/2011 de la Agencia Española de Protección de Datos:

  - El intercambio de información queda limitada a las operaciones de los artículos 18 y 19 de la LPBCYFT, y teniendo en cuenta lo apuntado anteriormente de *"….. cuando de las características u operativa del supuesto concreto se desprenda la posibilidad de que, una vez rechazada, pueda intentarse ante otros sujetos obligados*

el desarrollo de una operativa total o parcialmente similar a aquélla".

- El tratamiento quedará limitado expresamente a la única y exclusiva finalidad de *"prevenir o impedir operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo"*.
- Desde el punto de vista del acceso a los datos, el mismo deberá quedar limitado, conforme al artículo 33.4 LPBCYFT a *"los órganos de control interno previstos en el artículo 26 del mismo cuerpo legal, con inclusión de las unidades técnicas que constituyan los sujetos obligados ".*

En cuanto a la conservación de documentación, se establece la obligación de conservar durante un período mínimo de diez años la documentación en que se formalice el cumplimiento de las obligaciones establecidas en la LPBCYFT. Con las excepciones que se determinen por vía reglamentaria, se podrán almacenar las copias de los documentos de identificación en soportes ópticos, magnéticos o electrónicos que garanticen su integridad, la correcta lectura de los datos, la imposibilidad de manipulación y si adecuada conservación y localización.

Para concluir con este artículo quería poner de manifiesto que el Grupo de Trabajo del Artículo 29 desarrolló el Dictamen 14/2011, versado sobre la incidencia de la protección de datos personales en aspectos relacionados con la prevención del blanqueo de capitales y financiación del terrorismo, en el que hace constar su inquietud en estas materias. Al no disponer la LPBCYFT todavía de desarrollo reglamentario, nos preguntamos si ¿se reflejarán estas recomendaciones en el futuro reglamento o bien conllevarán la modificación de esta Ley?

Todo parece indicar que en breve saldremos de dudas pues según ha comunicado el propio Ministerio de Interior, el Reglamento verá la luz antes de lo que imaginamos.