

Protección de Datos Personales y Blanqueo de Capitales

Con la entrada en vigor de la Ley 10/20010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo -LBCFT-, la cual es de obligado cumplimiento a los sujetos encuadrados dentro del artículo 2 de la citada Ley, se abre un nuevo panorama de aplicación respecto a la normativa de protección de datos personales para dichos sujetos, en base a los preceptos que en aquella se disponen, especialmente, derivados del artículo 32 LBCFT.

La Ley de Blanqueo de Capitales y de la Financiación del Terrorismo efectúa importantes adiciones a la normativa de protección de datos personales para los sujetos obligados a cumplir aquella, los cuales son muchos. Pero, la afectación en protección de datos por la aplicación de la Ley de Blanqueo de Capitales ¿pudiere modificar considerablemente el grado de adecuación de las empresas o sujetos obligados al cumplimiento de aquella?

El presente artículo va dirigido a interpretar si dichos sujetos, por lo que se desprende del artículo 32 LBCFT se encuentran obligados a notificar ficheros exclusivos para cumplir con las obligaciones impuestas por LBCFT y a aplicar, por ende, las medidas de seguridad de nivel alto exigidas o, si por el contrario, no se ha de notificar fichero alguno adicional y exclusivo. Sin embargo, las exigencias que se incorporan a la LBCFT respecto a protección de datos, pudieren hacer pensar en que dichos sujetos obligados debieran proceder a cumplir con la obligación del artículo 96.1. párrafo 2º RDLOPD respecto a efectuar auditorías por dichos cambios en el sistema de información *“Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas.”*

Si analizamos, brevemente, la LBCFT es extenso el listado de obligados al cumplimiento de aquella: desde entidades de crédito y aseguradoras en la rama de vida, pasando por gestoras de fondos de pensiones, promotoras inmobiliarias y actividades de juego, llegando incluso a auditores de cuentas, asesores fiscales, notarios e inclusive a nuestra rama de actividad -abogados o procuradores en sus

actuaciones por cuentas de los clientes para supuestos de compra-venta de bienes inmuebles, valores, gestión de carteras o fondos, depósitos, etc.-

Dichos sujetos en sus operaciones, en su actividad diaria, en cuanto consideren que existen indicios, aunque sea una mera tentativa, de una actividad que pudiese dar lugar a blanqueo de capitales deben comunicarla al Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias. Para ello, dichos sujetos obligados deben disponer de controles internos establecidos al efecto para elaborar el denominado “examen especial” y, en caso que fuere necesario, comunicar al Servicio Ejecutivo de la Comisión la información que le es requerida, entre ella, la identificación de las personas intervinientes en la operación. De igual forma, la LBCFT obliga a que la documentación que se genere para dar cumplimiento a la citada normativa sea conservada, salvo excepciones, en soporte magnético, óptico o electrónico durante un período de 10 años y que la misma cumpla con los principios de integridad, autenticidad, conservación, localización y alteración

Por lo tanto, de las precedentes obligaciones se desprenden tres cosas: primera, la existencia de un tratamiento de información personal sujeta a la normativa de protección de datos personales; segunda, que existen comunicaciones de datos amparada por Ley a un organismo administrativo -Servicio Ejecutivo de la Comisión- que adelante adoptará la figura de encargado de tratamiento -artículo 32.4 LBCFT- y; tercera, la obligación de implantar un sistema de archivo y custodia, conllevando otros extremos: accesos, salidas, copias de seguridad, autorizaciones, y demás contempladas en el RDLOPD.

De igual forma, los sujetos obligados deben establecer procedimientos internos para controlar el blanqueo de capitales, estando obligados a establecer y documentar dicho procedimiento o manual, así como a designar representantes para efectuar las notificaciones ante el Servicio Ejecutivo de la Comisión. Eso no es todo, la propia LBCFT en su artículo 26.2 párrafo 3º in fine señala: *“Reglamentariamente se determinará para determinadas categorías de sujetos obligados la exigencia de constitución de unidades técnicas para el tratamiento y análisis de la información.”* De la obligación precedente, podemos hacernos varias cuestiones: ¿La redacción de la documental donde se detalle el procedimiento organizativo, técnico y legal -incluimos accesos, autorizaciones, manipulaciones, copias de seguridad, archivo y custodia, etc.- para cumplir con las obligaciones legales de la LBCFT valdrá como anexo o complemento al documento de seguridad? Dado que reglamentariamente se

establecerán las medidas que deben disponer esas unidades técnicas de tratamiento y análisis de información, ¿no afectará en sí al sistema de información y, por ende, a la exigencia de cumplir con el artículo 96 RDLOPD? A la primera de las cuestiones, mi opinión, es que no valdrá, dado que son leyes diferentes con un ámbito de aplicación distinto. Es lo mismo que el caso de encontrarse acreditado por la ISO 27000 y no por ello, cumpliendo con la normativa de protección de datos personales, a pesar que muchas de las exigencias de aquella son equiparables a las establecidas por la LOPD y RDLOPD. A la segunda de las cuestiones, mi pronunciamiento, es que la misma dará lugar a efectuar la auditoría correspondiente con la finalidad de conocer si las medidas implantadas cumplen con lo establecido en el RDLOPD.

Pasemos al artículo concreto de la LBCFT sobre protección de datos, es decir, el artículo 32 que destacaré varios extremos. El punto primero de dicho precepto dice: *“El tratamiento de datos de carácter personal, **así como los ficheros, automatizados o no, creados para el cumplimiento de las disposiciones de esta Ley** se someterán a lo dispuesto en la Ley Orgánica 15/1999 y su normativa de desarrollo.”* Nos encontramos con el primer “engorro”, relativo a si es obligatorio crear un fichero específico para cumplir con la Ley. Trataré de justificar mi conclusión, aunque me imagino que habrá posiciones en contrario, la cual es **NO ES NECESARIO NOTIFICAR UN NUEVO FICHERO EXCLUSIVO**. Ello, no significa que pudiere, en un determinado momento, ser aconsejable notificarlo, dado que puede resultar más factible aplicar las medidas organizativas y técnicas exigidas por la LBCFT para la información que el mismo se trata y almacena. ¿Por qué considero que no es necesaria una notificación adicional? Entiendo que la propia LBCFT solamente y expresamente habla de ficheros para ser creados los que aparecen en su propio articulado: Ficheros de Titularidades Financieras -artículo 43- los cuales deben obligatoriamente ser creados por las entidades de crédito; los Ficheros Centralizados para la Prevención del Fraude -artículo 33-, es decir, los que podríamos equiparar en el ámbito de la solvencia patrimonial y de crédito como los ficheros comunes donde las entidades adheridas pueden consultar información; y los Ficheros creados en los que se contengan datos personales o información de personas con responsabilidad pública -artículo 15.- Para el resto de casos, por ejemplo, el sujeto obligado que disponga de un fichero denominado CLIENTES notificado ante la AEPD y cumpliendo con las medidas técnicas, organizativas y legales establecidas en la normativa de protección de datos personales, pueden salvar la notificación aplicando el artículo 81.8 RDLOPD: *“A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o*

uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.” Considero que por aplicación, puede efectuarse una diferenciación de qué información contenida en el fichero CLIENTES le afecta por previsión legal la LBCFT y documentarlo en su correspondiente Documento de Seguridad indicando las medidas de seguridad aplicables a dicha segmentación. ¿Cuáles son esas medidas de seguridad? Pues las de nivel alto, como así señala el punto 5 del artículo 32 LBCFT: *“Serán de aplicación a los ficheros a los que se refiere este artículo las medidas de seguridad de nivel alto previstas en la normativa de protección de datos de carácter personal.”*

Por ello, aunque considere que no existe obligación expresa como tal para crear ficheros propios y exclusivos, sí, por el contrario, en un determinado momento, por la práctica, crearlo para establecer en el mismo dichas medidas de seguridad de nivel alto.

Para concluir, aunque el presente tema da para mucho más, indicar las peculiaridades adicionales de la LBCFT respecto a datos personales, destacando que no se pueden ejercer los derechos ARCO a dichos tipos de ficheros; ni se precisa consentimiento del afectado para tratar y almacenar la información personal para cumplir con las finalidades -obligaciones- marcadas o propias de la Ley; ni es necesario informar de los extremos contemplado en el artículo 5 LOPD. Esto último veremos si es extrapolable a los ficheros comunes.

Como conclusión y, para mí, la más importante, por lo menos la extraída, tras analizar la LBCFT es que la aplicación directa de ésta da lugar a la aplicación del artículo 96 del RDLOPD en cuanto a que, dado el nivel de seguridad es alto, las medidas a implantar en el sistema de información son considerables y, por ende, afectan, en la mayoría de los casos, a implantar medidas adicionales para tratar y almacenar la información contenida en los ficheros existentes o que se pudieren crear.

Efrén Santos Pascual

Socio-Abogado

ICEF Consultores