

La consulta pone de manifiesto que desde 2008 existe un Convenio de Colaboración suscrito entre la TGSS y ASNEF que regula el proceso de verificación de datos y cuyo objetivo fundamental es comprobar la veracidad de la información que las entidades recababan de sus clientes con ocasión del establecimiento de relaciones de negocio, a fin de conocer la naturaleza de su actividad profesional o empresarial con base en las exigencias establecidas por la normativa de prevención de blanqueo de capitales y financiación del terrorismo. En dicho Convenio se exige por la TGSS la recogida y custodia del consentimiento del cliente o potencial cliente por un plazo de dos años. No aporta el texto del convenio con su consulta. En esencia, pregunta si la figura del boqueo podría ser base jurídica suficiente para que las entidades financieras que forman parte de ASNEF custodien, y no supriman, el consentimiento que en virtud del convenio la TGSS exige a dichas entidades financieras que soliciten de sus clientes. Cita artículos de la normativa de blanqueo de capitales y del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).

En segundo lugar, expone el funcionamiento de la Central de Información de Riesgos del Banco de España (CIRBE) y que las entidades asociadas a ASNEF también consultan dicha base de datos para asesorarse del riesgo de crédito de los solicitantes de una operación financiera o para verificar datos en relación con las obligaciones impuestas por la normativa de blanqueo de capitales. Cita la normativa que regula dicha CIRBE, y finaliza preguntando, en definitiva, si la figura del bloqueo puede servir para que las entidades financieras puedan utilizar el bloqueo como base jurídica para conservar la solicitud firmada por el interesado en el que se le informa del derecho de la entidad financiera a consultar el CIRBE durante el período establecido en la norma.

Alternativamente, pregunta si podría entenderse que las obligaciones impuestas por la normativa de prevención del blanqueo de capitales y financiación del terrorismo justificarían la exclusión del derecho de supresión

(art. 17 RGPD) de los documentos citados (consentimiento e información) que soportan las mencionadas consultas, en base al cumplimiento de una obligación legal, conforme al nº 3, letra b), del mencionado art 17 RGPD.

I

El art. 4.2) del RGPD define «tratamiento» como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, **conservación**, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

Como puede verse, considera que la conservación de datos personales es un tratamiento de datos.

El art. 5.1, letra e) RGPD, dentro de los principios relativos al tratamiento, determina que los datos personales serán mantenidos de forma que se permita la identificación de los interesados **durante no más tiempo del necesario para los fines del tratamiento de los datos personales**; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

No se plantea aquí una cuestión de conservación con fines de archivo o para fines científicos, por lo que el principio citado obliga al responsable del tratamiento a conservar dichos datos durante no más tiempo del necesario para las finalidades para los que se recogieron.

De manera concordante con este principio, el art. 17 RGPD otorga a los interesados un derecho de supresión de sus datos personales, y correspondiente obligación para responsable de suprimir dichos datos, entre otras circunstancias cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo el

(letra b). Sin embargo, el propio RGPD prevé que dicho derecho puede tener limitaciones. El art. 17.3 RGPD establece que los apartados 1 y 2 [esto es, no habrá lugar a la supresión] no se aplicarán cuando el tratamiento sea necesario: b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

En interpretación de este apartado, el Considerando 65 RGPD dice así:

*(...) En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse **si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo**, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. (...) Sin embargo, **la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento**, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.*

En estos casos, la retención ulterior de dichos datos es lícita, dice el RGPD. Esto es, no concurriría un derecho del interesado a la supresión de los datos personales.

El art. 25 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, tras la redacción dada por el Real Decreto-ley 11/2018, de 31 de agosto, establece:

Artículo 25. Conservación de documentos.

*1. Los sujetos obligados **conservarán durante un período de diez años** la documentación en que se formalice el cumplimiento de las obligaciones establecidas en la presente ley, procediendo tras el mismo*

a su eliminación. Transcurridos cinco años desde la terminación de la relación de negocios o la ejecución de la operación ocasional, la documentación conservada únicamente será accesible por los órganos de control interno del sujeto obligado, con inclusión de las unidades técnicas de prevención, y, en su caso, aquellos encargados de su defensa legal.

En particular, los sujetos obligados conservarán para su uso en toda investigación o análisis, en materia de posibles casos de blanqueo de capitales o de financiación del terrorismo, por parte del Servicio Ejecutivo de la Comisión o de cualquier otra autoridad legalmente competente:

a) Copia de los documentos exigibles en aplicación de las medidas de diligencia debida, durante un periodo de diez años desde la terminación de la relación de negocios o la ejecución de la operación.

b) Original o copia con fuerza probatoria de los documentos o registros que acrediten adecuadamente las operaciones, los intervinientes en las mismas y las relaciones de negocio, durante un periodo de diez años desde la ejecución de la operación o la terminación de la relación de negocios.

2. Los sujetos obligados, con las excepciones que se determinen reglamentariamente, almacenarán las copias de los documentos de identificación a que se refiere el artículo 3.2 en soportes ópticos, magnéticos o electrónicos que garanticen su integridad, la correcta lectura de los datos, la imposibilidad de manipulación y su adecuada conservación y localización.

En todo caso, el sistema de archivo de los sujetos obligados deberá asegurar la adecuada gestión y disponibilidad de la documentación, tanto a efectos de control interno, como de atención en tiempo y forma a los requerimientos de las autoridades.

Esto es, impone a los sujetos obligados una obligación de conservación de determinados datos y documentos durante unos determinados plazos de tiempo. Esta obligación legal de conservación de documentos y las finalidades a las que sujeta su uso tras el plazo de cinco años a que se refiere el precepto determinan que el derecho de supresión del interesado se vea aquí desplazado por la ley.

Esto es, por otra parte, lo que establece el art. 32 de dicha ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, con relación a la protección de datos personales.

Artículo 32. Protección de datos de carácter personal.

(...)

3. En virtud de lo dispuesto en el artículo 24.1, y en relación con las obligaciones a las que se refiere el apartado anterior, no será de aplicación al tratamiento de datos la obligación de información prevista en el artículo 5 de la Ley Orgánica 15/1999.

Asimismo, **no serán de aplicación a los ficheros y tratamientos a los que se refiere este precepto las normas contenidas en la citada Ley Orgánica referidas al ejercicio de los derechos de acceso, rectificación, cancelación y oposición.** En caso de ejercicio de los citados derechos por el interesado, los sujetos obligados se limitarán a ponerle de manifiesto lo dispuesto en este artículo.

Lo dispuesto en el presente apartado será igualmente aplicable a los ficheros creados y gestionados por el Servicio Ejecutivo de la Comisión para el cumplimiento de las funciones que le otorga esta Ley.

(...)

En definitiva, la propia ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, exceptúa el derecho del interesado a la supresión de sus datos personales en ese contexto.

Por lo tanto, cabe concluir que la obligación legal impuesta a los sujetos obligados por la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo, de conservación de la documentación a que la ley 10/2010 hace referencia supone un tratamiento necesario para el cumplimiento de una obligación legal que cabe incluir dentro de la excepción al derecho de supresión previsto en el art. 17.3, letra b) del RGPD.

Ahora bien, esta excepción al derecho del interesado a la supresión de sus datos personales no supone ni mucho menos una excepción a que el sujeto obligado (la entidad financiera) debe de tratar los datos personales de conformidad con la normativa de protección de datos (véase el art. 32.1 de la propia ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo), por lo que seguirán siendo de aplicación los principios relativos al tratamiento previstos en el artículo 5 del RGPD, y entre ellos el principio de limitación de la finalidad (letra b); y sobre todo el principio de integridad y confidencialidad (letra f), que determina que dichos datos personales deberán ser tratados de tal manera que se garantice una seguridad

adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas.

En definitiva, dado que el art. 32 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales establece que el bloqueo es una obligación impuesta a los responsables del tratamiento cuando proceda la supresión de los datos, no procediendo en este caso, como se ha expuesto, la supresión de los datos, el bloqueo no puede ser considerado base jurídica suficiente para el mantenimiento de los datos por el responsable. Y ello, se añade para finalizar, sin perjuicio de que puedan adoptarse por el responsable del tratamiento aquellas medidas incluidas en la definición o descripción del bloqueo que se contiene en dicho artículo 32 como medidas técnicas y organizativas para la protección de los datos personales siempre que, ciertamente, dichas medidas no impidan los tratamientos que por obligación legal de la legislación de prevención de blanqueo de capitales se imponen a los sujetos obligados.