ECIJA
Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Nota informativa: Informe AEPD 2021/0047 sobre tratamiento de datos biométricos en procesos de video identificación en materia de Prevención de Blanqueo de Capitales

19 de Julio 2021

Recientemente se ha publicado por parte de la AEPD el Informe Jurídico en el que se analiza un proyecto que, en palabras de las AEPD, "plantea la viabilidad de realizar el tratamiento de datos biométricos para llevar a cabo el reconocimiento facial en el momento del alta de clientes en la oficina o a través de un canal online, con el objetivo de verificar su identidad y, de esta forma realizar las verificaciones oportunas previstas en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (PBC/FT), así como del control del fraude". En concreto, la consulta y el informe versa sobre las causas de legitimación que resultarían validas, en opinión de la AEPD, y específicamente sobre la utilización del consentimiento y/o el interés público como habilitación para el tratamiento descrito.

Mediante esta nota informativa, ECIJA analiza la interpretación de la AEPD y el impacto que el presente Informe puede conllevar respecto del cumplimiento del deber de diligencia debida en los procesos identificación obligatorios en materia de prevención de blanqueo de capitales y en otros ámbitos, tales como la emisión de certificados electrónicos cualificados mediante vídeo identificación, entre otros.

Cabe destacar que la AEPD no reproduce el contenido de la consulta sobre la que resuelve, por lo que son múltiples las dudas que surgen en cuanto al supuesto de hecho sobre el que se pronuncia y hasta qué punto sus conclusiones son extrapolables a otros supuestos semejantes a los planteados.

Quizá es esa falta del conocimiento en detalle del supuesto de hecho, el motivo de la inicial y sorprendente conclusión de este informe, que **descarta que sea posible amparar el tratamiento de datos biométricos en el consentimiento debidamente informado de forma previa de los interesados**, porque, según expone la AEPD, "*al tratarse de datos biométricos, es decir, de categorías especiales de datos, no puede ser una base jurídica adecuada por depender de que los clientes autoricen estos tratamientos. Y porque puede considerarse que un consentimiento obligatorio no sería lícito, al condicionar la prestación de servicios al otorgamiento del consentimiento con la consecuencia de que dicho consentimiento no sería libre*".

De forma general, el consentimiento es una de las bases de legitimación incluidas en el 9 del RGPD, para permitir el tratamiento de categorías especiales de datos personales y no se explica cuál es el motivo por el que no es aplicable su utilización y qué circunstancias concurren para considerar que el mismo, de forma absoluta, no es válido para esta tipología de tratamiento.

Aplicando la teoría general de contratos y los principios generales aplicables al consentimiento, la realidad es que la AEPD parece poner en duda la legalidad del uso del consentimiento por considerar que, en el supuesto planteado no existe alternativa para aquellos usuarios que no deseen prestar su consentimiento para este tipo de tratamiento, impidiendo así el acceso a los servicios financieros en cuestión, lo que sin duda alguna viciaría el consentimiento prestado, entendiéndose que si existiera alternativa para aquellos usuarios que deciden no prestar su consentimiento, sería un tratamiento que podría ampararse en el consentimiento debidamente informado.

Es precisamente, dicha información esencial que acompaña al consentimiento la que parece determinante en el tratamiento de datos biométricos o especialmente sensibles, de hecho, es determinante en todos los tratamientos de datos personales, en la medida en que lo realmente relevante en la teoría general de obligaciones y contratos, no es tanto la forma o el medio a través del que se preste el consentimiento, sino que la información previa y las condiciones bajo las que se preste el mismo, garanticen que éste no se encuentra viciado.

Ese es el hecho determinante para poder establecer si se trata de un consentimiento viciado o no, y así parece entenderlo el Reglamento General de Protección de Datos Personales, en tanto considera la autonomía de la voluntad, siempre que la misma se otorgue bajo la información previa suficiente y transparentes, así como las circunstancias adecuadas.

Adicionalmente, se anticipa que los datos biométricos tienen la consideración de categoría especial, volviendo la AEPD a retomar la teoría que ya hizo pública meses atrás en relación a la diferenciación entre dos conceptos determinantes: **autenticación** e **identificación**.

a) **Autenticación:** proceso en el que se realiza la autenticación de la identidad de un usuario utilizando los datos biométricos del mismo para compararlos contra otra fuente proporcionada por ese mismo usuario, considerada como una plantilla o documento de comparación (por ejemplo, comparación de los datos biométricos faciales, con la fotografía del DNI o el Pasaporte facilitado por el mismo usuario). Es lo que conoce como proceso de autenticación "uno a uno" (1 a 1).

b) **Identificación:** proceso en el que se realiza la identificación de un usuario utilizando los datos biométricos del mismo para compararlos con una multitud de patrones biométricos, de multiplicidad de individuos, almacenados en una o múltiples bases de datos, tratándose, por tanto, de un tratamiento de carácter masivo de datos personales de carácter biométrico. (por ejemplo, comparación de los datos biométricos faciales de un individuo, con una base de datos en la que existen miles de patrones biométricos obtenidos de otras personas). Es lo que conoce como proceso de autenticación "uno a varios" (1 a N).

En particular, para el caso planteado en la consulta analizada por la AEPD, ésta considera que nos encontramos dentro del segundo supuesto, un proceso de identificación propiamente dicho (uno a varios -1 a N-), y por tanto se trata de un proceso de identificación, teniendo la consideración de categoría especial de datos que suponen los datos biométricos.

No obstante, de nuevo, al no haberse aclarado el contenido y alcance del proyecto objeto de la consulta, tampoco existe una explicación de por qué se califica como identificación, y no autenticación, el proceso realizado.

En principio, el razonamiento lógico, y siguiendo los propios criterios de la AEPD, parece que ésta entiende que las labores perseguidas por parte de las entidad financiera que radiquen en dar cumplimiento a las obligaciones de diligencia debida en los procesos de identificación en materia de Prevención de Blanqueo de Capitales y Financiación de Terrorismo (PBCFT) y prevención del fraude, que no olvidemos, no es más que la prevención de la comisión de delitos tipificados por el Código Penal (para lo que es necesario realizar una identificación adecuada según el estado de la técnica existente en el momento concreto, siendo el uso de factores inherentes -como la biométria- los más eficaces para la prevención de la comisión de dichos delitos), en tanto se trata de procesos de autenticación (1 a 1) y no de procesos de identificación propiamente dichos (al menos no con los criterios por ella misma establecidos), seguirían siendo procesos perfectamente válidos.

Al igual que ocurre con el consentimiento, y en relación con los procesos de tratamiento de datos biométricos para realizar procesos de identificación (1 a N), la AEPD niega la posibilidad de amparar este tratamiento en la existencia de un interés público.

Tras un largo razonamiento jurídico en el que condiciona la existencia de este interés a que el mismo esté expresamente reconocido en una norma con rango de Ley que delimite de forma concreta los límites al derecho a la protección de datos personales, considera que este no concurre en relación con lo regulado en la ley de PBCFT "*ya que el legislador no ha previsto el uso de datos biométricos como una medida proporcional para la identificación de las personas físicas, estableciendo las garantías específicas y adecuadas que se derivan de los mayores riesgos que implica el tratamiento de dichos datos*".

En consecuencia, la AEPD únicamente considera proporcional llevar a cabo un proceso de autenticación (según el concepto anteriormente indicado), en el que se compruebe mediante los documentos fehacientes aportados por éste y la cara del individuo en cuestión que los aporta, pareciendo obviar en esta valoración, las medidas y controles requeridas en las distintas Instrucciones publicadas por SEPBLAC para llevar a cabo los procesos de video-identificación asistida y desasistida, en las que expresamente hace referencia a la responsabilidad del sujeto obligado en relación a la implantación de "*los requerimientos técnicos que permitan verificar la autenticidad, vigencia e integridad de los documentos de identificación utilizados y la correspondencia del titular del documento con el cliente objeto de vídeo-identificación*".

En particular, las instrucciones referidas publicadas en el año 2016 y 2017 por parte del Servicio de Prevención de Blanqueo de Capitales (SEPBLAC) y debidamente justificadas en virtud de lo dispuesto en el artículo 21.1d) del Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (RPBCFT), en el que se dispone que será posible realizar la identificación del cliente de forma no presencial, cumplimiento con el deber de diligencia debida, siempre que ***"****La identidad del cliente quede acreditada mediante el empleo de otros procedimientos seguros de identificación de clientes en operaciones no presenciales,* ***siempre que tales procedimientos hayan sido previamente autorizados por el***

Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias"

Sorprende que esta disposición legal, y las referidas instrucciones del SEPBLAC no sean, si quiera, tenidas en consideración a la hora de analizar la posibilidad del uso de la biometría en los procesos de autenticación y/o identificación no presencial, que aunque no sea expresamente mencionada en la norma es, de facto, la única tecnología viable a día de hoy para permitir una identificación segura, distinta de la expresamente regulada en el referido artículo 21 (firma electrónica cualificada, intervención de fedatario público o preexistencia de una cuenta abierta en un país con garantías suficientes).

Estamos seguros de que el SEPBLAC habría estado muy interesado en conocer, antes de la publicación del citado informe publicado por la AEPD, sus conclusiones respecto a los procesos de identificación seguros y robustos, que desde hace bastantes años han permitido reducir, con creces, el número de operaciones fraudulentas relacionadas con blanqueo de capitales y financiación de terrorismo, así como la lucha contra bandas criminales organizadas especializadas en la comisión de fraudes financieros.

Sobre este particular debe tenerse en cuenta que, además en relación con la identificación en procesos de emisión de certificados conforme al Reglamento (UE) n.º 910/2014 (e-IDAS) y su normativa de desarrollo, la reciente aprobación de la Orden Ministerial ETD/465/2021 "sobre los métodos de identificación no presencial para la expedición de certificado electrónicos cualificados", emitida el 6 de mayo de 2021 por el Ministerio de Asuntos Económicos y Transformación Digital y la posterior aprobación del esquema de certificación y auditoría de cumplimiento publicado por el Centro Criptológico Nacional, hacen referencia específica a la utilización de factores de inherencia para dar cumplimiento, y dotar del mayor grado de seguridad, a los proceso de identificación no presencial para la emisión de certificados electrónicos cualificados.

Sin embargo, la AEPD en el presente Informe concluye que no puede legitimarse el tratamiento, ni en el consentimiento del cliente, ni en el interés público alegado, estableciendo expresamente que "*el DNI acredita por si solo y a todos los efectos la identidad y los datos personales de su titular. De este modo, el imponer como obligatoria la identificación mediante reconocimiento facial no se ajustaría a lo previsto en la normativa vigente, además de ser desproporcionado,etc*", sin entrar a valorar si podría ser viable, amparado expresamente en lo dispuesto en RGPD, en el interés legítimo de la lucha y prevención contra el fraude o en el mero cumplimiento normativo, haciendo referencia a toda la normativa referida previamente en materia de PBCFT.

El contenido, interpretaciones y conclusiones del Informe de la AEPD se encuentran del todo alejados de la realidad operativa, tecnológica, y normativa implantada para el cumplimiento de las exigencias legales establecidas en materia de identificación para la prevención del fraude y el blanqueo de capitales, específicamente respecto de los procesos de identificación efectuados de forma remota, en el que el establecimiento de medidas que permitan la verificación del documento de identificación fehaciente utilizado se corresponde inequívocamente al sujeto (persona física titular) que está realizando el trámite de identificación es esencial para minorar los riesgos de suplantación de identidad, que, de otro modo, no sería posible ejecutar, dando alas, sin que parezca que lo tenga ni siquiera en

cuenta, a la imponentes mafias organizadas que día a día intentan poner en jaque todo tipo de negocios, tanto en ámbitos financieros, como en el de las telecomunicaciones, energía y en general, todos los servicios de carácter masivo que permiten, por petición expresa de sus usuarios en muchos casos, la posibilidad de realizar las contrataciones no presenciales, para las que se requiere siempre la identificación previa.

En este sentido, y en relación con el informe 47/2021, sobre reconocimiento facial para la identificación de personas en base a la normativa sobre PBC objeto de la presente Nota, cabe interpretar que no es que dicho reconocimiento facial no se pueda realizar, sino que la posibilidad de llevarse a cabo va a depender, en gran medida, del consentimiento libre y expreso del interesado, consentimiento que pasa por el ofrecimiento al interesado de métodos alternativos para identificarse (impidiendo que se vicie el consentimiento), aspecto este que podría cubrirse fácilmente en la identificación en oficina mediante los documentos acreditativos fehacientes reconocidos y la verificación por el empleado de la correspondencia con la persona titular del mismo, pero no encuentra el mismo soporte respecto de las identificaciones realizadas a distancia, donde esta tecnología se ha demostrado del todo eficaz en la disminución de fraude y la suplantación de identidad.

Adicionalmente no parece tenerse en cuenta tampoco por la AEPD la importancia de la homogeneización de procesos en el cumplimiento de las obligaciones legales de las entidades, ni la coordinación con otros organismos reguladores de ámbito nacional, independientemente del canal por el que se efectúen estas, pues son la base para la acreditación de la diligencia debida de los responsables ante requerimientos y solicitudes tanto de los distintos organismos de control, como por parte de los usuarios ante posibles reclamaciones.

Ante la inseguridad jurídica que genera un informe de este tipo, y teniendo el riesgo asociado a la limitación que se puede producir en relación con el uso de una tecnología que está llamada a ser un factor clave en la lucha contra el blanqueo de capitales y financiación del terrorismo, así como contra cualquier tipo de fraude asociado a la suplantación de identidad, muy especialmente en las operaciones realizadas a distancia, no cabe más que esperar que el legislador intervenga lo antes posible para establecer un marco legal que regule de forma expresa y en norma de rango de ley las posibilidades del uso de tecnología biométrica, de modo que todos los actores afectados cuenten con pautas claras para utilizarla, pues ha quedado acreditado que el uso de estos sistemas contribuyen a obstaculizar las acciones de aquellos que pretenden saltarse los controles de seguridad, sin que su uso suponga la persistente amenaza de una potencial sanción por incumplimiento de otras normativas relacionadas en base a las interpretaciones dispares de los distintos organismos de control. ,

Quedamos a su disposición para cualquier duda o cuestión que pudiera surgir.

Reciba un cordial un saludo,

Área de Privacidad y IT Compliance de ECIJA
info@ecija.com
Telf: + 34 91.781.61.60