N/REF: 0047/2021

El proyecto plantea el tratamiento de datos de 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 así 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.

El proyecto presentado se limita a:

- Señalar que la base jurídica del consentimiento para el tratamiento de los datos, 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.

- La alternativa al consentimiento que se propone es la de considerar como base jurídica para el tratamiento de datos sin consentimiento el cumplimiento de una misión de interés público cómo es la prevención del blanqueo de capitales y la financiación del terrorismo. Estando limitada la aplicación de esta base jurídica exclusivamente a los fines indicados y no a fines comerciales o de cualquier otro tipo distinto del control del fraude o de la PBC/FT.

I

El 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) define en su artículo 4.14 los datos biométricos como “datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos”.

El artículo 9 de dicha norma regula el tratamiento de categorías especiales de datos, entre los que se encuentran los datos biométricos,

estableciendo una prohibición general de su tratamiento en los siguientes términos:

"Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física."

En relación con el tratamiento de datos de reconocimiento facial, en nuestro Informe 36/2020, analizando el artículo 9.1 en relación con el Considerando 51 del RGPD, así como el Protocolo de enmienda al Convenio para la Protección de Individuos con respecto al procesamiento de datos personales, aprobada por el Comité de Ministros en su 128º período de sesiones en Elsinore el 18 de mayo de 2018 (Convenio 108+) señalábamos que

> *"Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía el Grupo del Artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas:*
>
> *Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).*
>
> *Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).*
>
> *Esta misma diferenciación se recoge en el Libro blanco sobre la inteligencia artificial de la Comisión Europea:*
>
> *"En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la*

misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos".

Atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).

No obstante, esta Agencia considera que se trata de una cuestión compleja, sometida a interpretación, respecto de la cual no se pueden extraer conclusiones generales, debiendo atenderse al caso concreto según los datos tratados, las técnicas empleadas para su tratamiento y la consiguiente injerencia en el derecho a la protección de datos, debiendo, en tanto en cuanto no se pronuncia al respecto el Comité Europeo de Protección de Datos o los órganos jurisdiccionales, adoptarse, en caso de duda, la interpretación más favorable para la protección de los derechos de los afectados."

Por consiguiente, en dicho informe esta Agencia destacaba ya la dificultad de deslindar los conceptos de identificación y autenticación, lo que requiere estar al caso concreto y a las particulares técnicas empleadas en relación con la finalidad perseguida por el tratamiento, así como la necesidad de otorgar la máxima protección a los derechos de los afectados frente al uso de técnicas que puede ser más invasivas para su privacidad y generar mayores riesgos para sus derechos y libertades.

En el proyecto presentado se realiza un de tratamiento de datos biométricos con la finalidad de cumplir con el deber de identificación establecido en la normativa sobre prevención del blanqueo de capitales y financiación del terrorismo, evitando, de este modo, la posible suplantación de identidad. Por consiguiente, debe concluirse que el proceso de reconocimiento facial empleado implica el tratamiento de datos biométricos con la finalidad de identificar unívocamente a una persona física, por lo que es un tratamiento de categorías especiales de datos sujeto a la regla general de prohibición de los mismos (art. 9.1. RGPD).

Esta misma conclusión alcanzó la Agencia en el citado informe 36/2020, analizando un supuesto análogo al presente, en el que lo que se pretendía era la identificación mediante el reconocimiento facial de los alumnos que realizaban los exámenes en la modalidad on line, al objeto de verificar su identidad y evitar supuestos de suplantación.

No obstante, el artículo 9.2 del RGPD regula excepciones a dicha prohibición general al establecer que

> "el apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
>
> a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado.
>
> (…)
>
> g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;"

En relación con el apartado g), destaca que cuando el tratamiento sea necesario por razones de interés público, que debe ser esencial sobre la base del derecho de los Estados miembros, proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. Procede, por consiguiente, analizar si, en el presente caso, concurren los presupuestos establecidos en el artículo 9.2.g) para levantar la prohibición de tratamiento de datos biométricos.

II

Esta Agencia ha tenido ocasión de pronunciarse, en diversas ocasiones, respecto de los requisitos establecidos por el artículo 9.2.g) del RGPD para poder amparar los tratamientos de datos personales basados en el reconocimiento facial, dada la proliferación de propuestas recibidas en relación con los mismos desde ámbitos diferentes, lo que pone de manifiesto el interés creciente en utilizar estos sistemas y la constante preocupación de esta autoridad de control, al tratarse de sistemas de identificación muy intrusivos para los derechos y libertades fundamentales de las personas físicas. Preocupación que es compartida por el resto de autoridades de control desde hace años, como ponen de manifiesto el Documento de trabajo sobre biometría, adoptado el 1 de agosto de 2003 por el Grupo del 29, o el posterior Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, adoptado el 27 de abril de 2012, y que ha llevado a que el propio legislador comunitario incluya estos datos entre las categorías especiales de datos en el RGPD. De este modo, estando prohibido su tratamiento con carácter general, cualquier excepción a dicha prohibición habrá de ser objeto de interpretación restrictiva.

A este respecto, cabe destacar, además del citado informe 36/2020, referido al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online, el informe 31/2019 sobre la incorporación de sistemas de reconocimiento facial en los servicios de videovigilancia al amparo del artículo 42 de la Ley de Seguridad Privada o el Informe 97/2020 relativo al Proyecto de Orden de la Ministra de Asuntos Económicos y Transformación Digital sobre los métodos de identificación no presencial para la expedición de certificados electrónicos cualificados. En todos estos casos se concluía que no existía norma legal en el ordenamiento jurídico español que reuniera los requisitos del artículo 9.2.g) del RGPD, por lo que el tratamiento únicamente podría ampararse en el consentimiento de los afectados siempre que quedara garantizado que el mismo es libre.

Analizando los requisitos del artículo 9.2.g) en nuestro Informe 36/2020 señalábamos lo siguiente:

V

La siguiente cuestión que se plantea en la consulta es si el tratamiento de los datos biométricos por los sistemas de reconocimiento facial en los procesos de evaluación online podría ampararse en la existencia de un interés público esencial conforme al artículo 9.2.g) del RGPD:

> *g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.*

Tal y como señalábamos anteriormente, el tratamiento de datos personales necesarios para la prestación del servicio público de educación superior se legitima, con carácter general, en la existencia de un interés público al amparo de lo previsto en el artículo 6.1.e) del RGPD. Sin embargo, tratándose de categorías especiales de datos, el supuesto contemplado en la letra g) del artículo 9.2. no se refiere solo a la existencia de un interés público, tal y como hace en muchos otros de sus preceptos el RGPD, sino que es el único precepto del RGPD que requiere que el mismo sea "esencial", adjetivo que viene a cualificar dicho interés público, habida cuenta de la importancia y necesidad de mayor protección de los datos tratados.

Dicho precepto encuentra su precedente en el artículo 8.4 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al

tratamiento de datos personales y a la libre circulación de estos datos: "4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control". No obstante, de su lectura resulta un mayor rigor en a nueva regulación por el RGPD, ya que se sustituye el adjetivo "importantes" por "esencial" y no se permite que la excepción pueda establecerse por las autoridades de control.

En relación con lo que debe entenderse por interés público esencial, debe tenerse igualmente en cuenta la Jurisprudencia del Tribunal Europeo de Derechos Humanos, que al amparo del artículo 8 del Convenio Europeo de Derechos Humanos, viene considerando que el tratamiento de datos personales constituye una injerencia lícita en el derecho del respeto de la vida privada y sólo puede llevarse a cabo si se realiza de conformidad con la ley, sirve a un fin legítimo, respeta la esencia de los derechos y libertades fundamentales y es necesario y proporcionado en una sociedad democrática para alcanzar un fin legítimo (D.L. contra Bulgaria, nº 7472/14, 19 de mayo de 2016, Dragojević contra Croacia, nº 68955/11, 15 de enero de 2015, Peck contra Reino Unido, nº 44647/98, 28 de enero de 2003, Leander contra Suecia, n.o 9248/81, 26 de marzo de 1987, entre otras). Como señala en la última sentencia citada, «el concepto de necesidad implica que la injerencia responda a una necesidad social acuciante y, en particular, que sea proporcionada con el fin legítimo que persigue».

Asimismo, debe tenerse en cuenta la doctrina del Tribunal Constitucional respecto a las restricciones al derecho fundamental a la protección de datos, que sintetiza en su sentencia 292/2000, de 30 de noviembre, en la que después de configurar el derecho fundamental a la protección de datos personales como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso, analiza los límites del mismo, señalando en lo siguiente:

> *Más concretamente, en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el*

principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7; 196/1987, de 11 de diciembre [RTC 1987, 196] , F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero [RTC 1994, 57] , F. 6; 18/1999, de 22 de febrero [RTC 1999, 18] , F. 2).

Justamente, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen. Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos

fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional […]". (Fundamento Jurídico 11)

"De un lado, porque si bien este Tribunal ha declarado que la Constitución no impide al Estado proteger derechos o bienes jurídicos a costa del sacrificio de otros igualmente reconocidos y, por tanto, que el legislador pueda imponer limitaciones al contenido de los derechos fundamentales o a su ejercicio, también hemos precisado que, en tales supuestos, esas limitaciones han de estar justificadas en la protección de otros derechos o bienes constitucionales (SSTC 104/2000, de 13 de abril [RTC 2000, 104] , F. 8 y las allí citadas) y, además, han de ser proporcionadas al fin perseguido con ellas (SSTC 11/1981, F. 5, y 196/1987, F. 6). Pues en otro caso incurrirían en la arbitrariedad proscrita por el art. 9.3 CE.

De otro lado, aun teniendo un fundamento constitucional y resultando proporcionadas las limitaciones del derecho fundamental establecidas por una Ley (STC 178/1985 [RTC 1985, 178]), éstas pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación. Conclusión que se corrobora en la jurisprudencia del Tribunal Europeo de Derechos Humanos que ha sido citada en el F. 8 y que aquí ha de darse por reproducida. Y ha de señalarse, asimismo, que no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), concebida como certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho (STC 104/2000, F. 7, por todas), sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, F. 15; 142/1993, de 22 de abril [RTC 1993, 142] , F. 4, y 341/1993, de 18 de noviembre [RTC 1993, 341] , F. 7). De suerte que la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción. Y al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja

que en su lugar opere simplemente la voluntad de quien ha de aplicarla, menoscabando así tanto la eficacia del derecho fundamental como la seguridad jurídica […]". (FJ 15).

"Más concretamente, en relación con el derecho fundamental a la intimidad hemos puesto de relieve no sólo la necesidad de que sus posibles limitaciones estén fundadas en una previsión legal que tenga justificación constitucional y que sean proporcionadas (SSTC 110/1984, F. 3, y 254/1993, F. 7) sino que la Ley que restrinja este derecho debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora. De no ser así, mal cabe entender que la resolución judicial o el acto administrativo que la aplique estén fundados en la Ley, ya que lo que ésta ha hecho, haciendo dejación de sus funciones, es apoderar a otros Poderes Públicos para que sean ellos quienes fijen los límites al derecho fundamental (SSTC 37/1989, de 15 de febrero [RTC 1989, 37], y 49/1999, de 5 de abril [RTC 1999, 49]).

De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación. […] (FJ 16)".

Asimismo, nuestro Tribunal Constitucional ha tenido ya la ocasión de pronunciarse específicamente sobre el artículo 9.2.g) del RGPD, como consecuencia de la impugnación del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, introducido por la disposición final tercera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, relativo a la legitimación de la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales, precepto que fue declarado inconstitucional por la Sentencia num. 76/2019 de 22 mayo.

Dicha sentencia analiza, en primer término, el régimen jurídico al que se encuentra sometido el tratamiento de las categorías especiales de datos en el RGPD:

> *De acuerdo con el apartado 1 del art. 9 RGPD, está prohibido el tratamiento de datos personales que revelen las opiniones políticas, del mismo modo que lo está el tratamiento de datos personales que revelen el origen étnico o racial, las convicciones religiosas o filosóficas o la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. No obstante, el apartado 2 del mismo precepto autoriza el tratamiento de todos esos datos cuando concurra alguna de las diez circunstancias allí previstas [letras a) a j)]. Algunas de esas circunstancias tienen un ámbito de aplicación acotado (laboral, social, asociativo, sanitario, judicial, etc.) o responden a una finalidad determinada, por lo que, en sí mismas, delimitan los tratamientos específicos que autorizan como excepción a la regla general. Además, la eficacia habilitante de varios de los supuestos allí previstos está condicionada a que el Derecho de la Unión o el de los Estados miembros los prevean y regulen expresamente en su ámbito de competencias: es el caso de las circunstancias recogidas en las letras a), b), g), h), i) y j).*
>
> *El tratamiento de las categorías especiales de datos personales es uno de los ámbitos en los que de manera expresa el Reglamento General de Protección de Datos ha reconocido a los Estados miembros "margen de maniobra" a la hora de "especificar sus normas", tal como lo califica su considerando 10.* ***Este margen de configuración legislativa se extiende tanto a la determinación de las causas habilitantes para el tratamiento de datos personales especialmente protegidos -es decir, a la identificación de los fines de interés público esencial y la apreciación de la proporcionalidad del tratamiento al fin perseguido, respetando en lo esencial el derecho a la protección de datos- como al establecimiento de "medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" [art. 9.2 g) RGPD]. El Reglamento contiene, por tanto, una obligación concreta de los Estados miembros de establecer tales garantías, en el caso de que habiliten para tratar los datos personales especialmente protegidos.***

En relación con el primero de los requisitos exigidos por el artículo 9.2.g), la invocación de un interés público esencial y la necesaria especificación del mismo, el Alto Tribunal recuerda lo señalado en su

sentencia 292/2000 en la que se rechazaba que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas, considerando que la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público" :

> *En la ya citada STC 292/2000 (RTC 2000, 292) , en la que también se enjuició una injerencia legislativa en el derecho a la protección de datos personales, rechazamos que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas:*
> *"16. [...] De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación.*
> *17. En el caso presente, el empleo por la LOPD (RCL 2018, 1629) en su art. 24.1 de la expresión "funciones de control y verificación", abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia. De un lado, al habilitar la LOPD a la Administración para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo. Y de un modo tal que, como señala el Defensor del Pueblo, permite reconducir a las mismas prácticamente toda actividad administrativa, ya que toda actividad administrativa que implique entablar una relación jurídica con un administrado, que así será prácticamente en todos los casos en los que la Administración necesite de datos personales de alguien, conllevará de ordinario la potestad de la Administración de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración. Lo que, a la vista del motivo de restricción del derecho a ser informado del art. 5 LOPD, deja en la más*

absoluta incertidumbre al ciudadano sobre en qué casos concurrirá esa circunstancia (si no en todos) y sume en la ineficacia cualquier mecanismo de tutela jurisdiccional que deba enjuiciar semejante supuesto de restricción de derechos fundamentales sin otro criterio complementario que venga en ayuda de su control de la actuación administrativa en esta materia.

Iguales reproches merece, asimismo, el empleo en el art. 24.2 LOPD de la expresión "interés público" como fundamento de la imposición de límites a los derechos fundamentales del art. 18.1 y 4 CE, pues encierra un grado de incertidumbre aún mayor. Basta reparar en que toda actividad administrativa, en último término, persigue la salvaguardia de intereses generales, cuya consecución constituye la finalidad a la que debe servir con objetividad la Administración con arreglo al art. 103.1 CE."

Esta argumentación es plenamente trasladable al presente enjuiciamiento. De igual modo, por tanto, debemos concluir que la legitimidad constitucional de la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público". Pues en otro caso el legislador habría trasladado a los partidos políticos -a quienes la disposición impugnada habilita para recopilar datos personales relativos a las opiniones políticas de las personas en el marco de sus actividades electorales- el desempeño de una función que solo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente sus límites y su regulación.

Tampoco puede aceptarse, por igualmente imprecisa, la finalidad aducida por el abogado del Estado, que se refiere al funcionamiento del sistema democrático, pues también encierra un grado elevado de incertidumbre y puede suponer un razonamiento circular. Por un lado, los partidos políticos son de por sí "cauces necesarios para el funcionamiento del sistema democrático" (por todas, STC 48/2003, de 12 de marzo (RTC 2003, 48) , FJ 5); y, por otro lado, todo el funcionamiento del sistema democrático persigue, en último término, la salvaguardia de los fines, valores y bienes constitucionales, pero ello no alcanza a identificar la razón por la cual haya de restringirse el derecho fundamental afectado.

Finalmente, debe precisarse que no es necesario que se pueda sospechar, con mayor o menor fundamento, que la restricción persiga una finalidad inconstitucional, o que los datos que se recopilen y procesen resultarán lesivos para la esfera privada y el ejercicio de los derechos de los particulares. Es suficiente con constatar que, al no poderse identificar con la suficiente precisión la finalidad del tratamiento de datos, tampoco puede enjuiciarse el

carácter constitucionalmente legítimo de esa finalidad, ni, en su caso, la proporcionalidad de la medida prevista de acuerdo con los principios de idoneidad, necesidad y proporcionalidad en sentido estricto.

Por otro lado, en cuanto a las garantías que debe adoptar el legislador, la citada sentencia núm. 76/2019 de 22 mayo, después de recordar que "A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental", analiza cuál es la norma que debe contener las citadas garantías:

"Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y regula ese uso o pueden encontrarse también en otras fuentes normativas.

La cuestión solo puede tener una respuesta constitucional. La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del art. 53.1 CE (RCL 1978, 2836) para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales.

Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas -unas veces- de predeterminación normativa y -otras- de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de

medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares" (FJ 8).

Por consiguiente, el tratamiento de datos biométricos al amparo del artículo 9.2.g) requiere que esté previsto en una norma de derecho europeo o nacional, debiendo tener en este último caso dicha norma, según la doctrina constitucional citada y lo previsto en el artículo 9.2 de la LOPDGDD, rango de ley. Dicha ley deberá, además especificar el interés público esencial que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, estableciendo las reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, sin que sea suficiente, a estos efectos, la invocación genérica de un interés público. Y dicha ley deberá establecer, además, las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, *tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:*

"En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo [RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [RTC 2000, 186] , F. 6)."

En el presente caso, dicho tratamiento pretende ampararse en la obligación de identificación que impone a los sujetos obligados el artículo 3 de la Ley 10/2010 de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo:

> Artículo 3. Identificación formal.
>
> 1. Los sujetos obligados identificarán a cuantas personas físicas o jurídicas pretendan establecer relaciones de negocio o intervenir en cualesquiera operaciones.
>
> En ningún caso los sujetos obligados mantendrán relaciones de negocio o realizarán operaciones con personas físicas o jurídicas que no hayan sido debidamente identificadas. Queda prohibida, en particular, la apertura, contratación o mantenimiento de cuentas, libretas de ahorro, cajas de seguridad, activos o instrumentos numerados, cifrados, anónimos o con nombres ficticios.
>
> 2. Con carácter previo al establecimiento de la relación de negocios o a la ejecución de cualesquiera operaciones, los sujetos obligados comprobarán la identidad de los intervinientes mediante documentos fehacientes. En el supuesto de no poder comprobar la identidad de los intervinientes mediante documentos fehacientes en un primer momento, se podrá contemplar lo establecido en el artículo 12, salvo que existan elementos de riesgo en la operación.
>
> Reglamentariamente se establecerán los documentos que deban reputarse fehacientes a efectos de identificación.
>
> 3. En el ámbito del seguro de vida, la comprobación de la identidad del tomador deberá realizarse con carácter previo a la celebración del contrato. La comprobación de la identidad del beneficiario del seguro de vida deberá realizarse en todo caso con carácter previo al pago de la prestación derivada del contrato o al ejercicio de los derechos de rescate, anticipo o pignoración conferidos por la póliza.

Como puede observarse, el citado precepto establece una obligación de identificación, estableciendo, asimismo, la forma en la que se debe proceder a la misma: “mediante documentos fehacientes”, remitiéndose a la normativa reglamentaria al objeto de determinar “los documentos que deban reputarse fehacientes”.

A este respecto, el 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, determina dichos documentos en su artículo 6:

> Artículo 6. Documentos fehacientes a efectos de identificación formal.
>
> 1. Se considerarán documentos fehacientes, a efectos de identificación formal, los siguientes:
>
> a) Para las personas físicas de nacionalidad española, el Documento Nacional de Identidad.
>
> Para las personas físicas de nacionalidad extranjera, la Tarjeta de Residencia, la Tarjeta de Identidad de Extranjero, el Pasaporte o, en el caso de ciudadanos de la Unión Europea o del Espacio Económico Europeo, el documento, carta o tarjeta oficial de identidad personal expedido por las autoridades de origen. Será asimismo documento válido para la identificación de extranjeros el documento de identidad expedido por el Ministerio de Asuntos Exteriores y de Cooperación para el personal de las representaciones diplomáticas y consulares de terceros países en España.
>
> Excepcionalmente, los sujetos obligados podrán aceptar otros documentos de identidad personal expedidos por una autoridad gubernamental siempre que gocen de las adecuadas garantías de autenticidad e incorporen fotografía del titular.
>
> b) Para las personas jurídicas, los documentos públicos que acrediten su existencia y contengan su denominación social, forma jurídica, domicilio, la identidad de sus administradores, estatutos y número de identificación fiscal.
>
> En el caso de personas jurídicas de nacionalidad española, será admisible, a efectos de identificación formal, certificación del Registro Mercantil provincial, aportada por el cliente u obtenida mediante consulta telemática.
>
> 2. En los casos de representación legal o voluntaria, la identidad del representante y de la persona o entidad representada, será comprobada documentalmente. A estos efectos, deberá obtenerse copia del documento fehaciente a que se refiere el apartado precedente correspondiente tanto al representante como a la persona o entidad representada, así como el documento público acreditativo de los poderes conferidos. Será admisible la comprobación mediante certificación del Registro Mercantil provincial, aportada por el cliente, u obtenida mediante consulta telemática.

3. Los sujetos obligados identificarán y comprobarán mediante documentos fehacientes la identidad de todos los partícipes de las entidades sin personalidad jurídica. No obstante, en el supuesto de entidades sin personalidad jurídica que no ejerzan actividades económicas bastará, con carácter general, con la identificación y comprobación mediante documentos fehacientes de la identidad de la persona que actúe por cuenta de la entidad.

En el supuesto de fondos de inversión, la obligación de identificación y comprobación de la identidad de los partícipes se realizará conforme a lo dispuesto en el artículo 40.3 de la Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva.

En los fideicomisos anglosajones («trusts») u otros instrumentos jurídicos análogos que, no obstante carecer de personalidad jurídica, puedan actuar en el tráfico económico, los sujetos obligados requerirán el documento constitutivo, sin perjuicio de proceder a la identificación y comprobación de la identidad de la persona que actúe por cuenta de los beneficiarios o de acuerdo con los términos del fideicomiso, o instrumento jurídico. A estos efectos, los fideicomisarios comunicarán su condición a los sujetos obligados cuando, como tales, pretendan establecer relaciones de negocio o intervenir en cualesquiera operaciones. En aquellos supuestos en que un fideicomisario no declare su condición de tal y se determine esta circunstancia por el sujeto obligado, se pondrá fin a la relación de negocios, procediendo a realizar el examen especial a que se refiere el artículo 17 de la Ley 10/2010, de 28 de abril.

4. Los documentos de identificación deberán encontrarse en vigor en el momento de establecer relaciones de negocio o ejecutar operaciones ocasionales. En el supuesto de personas jurídicas, la vigencia de los datos consignados en la documentación aportada deberá acreditarse mediante una declaración responsable del cliente.

Por otro lado, el artículo 13 prevé otros medios de identificación, sin perjuicio de que deban obtenerse, igualmente, los correspondientes documentos fehacientes:

Artículo 12. Relaciones de negocio y operaciones no presenciales.

1. Los sujetos obligados podrán establecer relaciones de negocio o ejecutar operaciones a través de medios telefónicos, electrónicos o telemáticos con clientes que no se encuentren físicamente presentes, siempre que concurra alguna de las siguientes circunstancias:

a) La identidad del cliente quede acreditada mediante la firma electrónica cualificada regulada en el Reglamento (UE) n.º 910/2014 del

Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. En este caso no será necesaria la obtención de la copia del documento, si bien será preceptiva la conservación de los datos de identificación que justifiquen la validez del procedimiento.

b) El primer ingreso proceda de una cuenta a nombre del mismo cliente abierta en una entidad domiciliada en España, en la Unión Europea o en países terceros equivalentes.

c) Se verifiquen los requisitos que se determinen reglamentariamente.

En todo caso, en el plazo de un mes desde el establecimiento de la relación de negocio, los sujetos obligados deberán obtener de estos clientes una copia de los documentos necesarios para practicar la diligencia debida.

Cuando se aprecien discrepancias entre los datos facilitados por el cliente y otra información accesible o en poder del sujeto obligado, será preceptivo proceder a la identificación presencial.

Los sujetos obligados adoptarán medidas adicionales de diligencia debida cuando en el curso de la relación de negocio aprecien riesgos superiores al riesgo promedio.

2. Los sujetos obligados establecerán políticas y procedimientos para afrontar los riesgos específicos asociados con las relaciones de negocio y operaciones no presenciales.

No obstante, el uso de dichos medios queda condicionado al posible riesgo de la operación, tal y como señala el artículo 3 de la LPBCFT. Precisamente, la valoración del riesgo es un elemento central en la normativa sobre prevención del blanqueo de capitales y financiación del terrorismo.

De la regulación transcrita, que es transposición de la normativa comunitaria, fácilmente puede colegirse que la misma no cumple con los requisitos establecidos en el artículo 9.2.g), 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.

Por consiguiente, pretendiéndose en el proyecto el tratamiento de datos personales incluidos en las categorías especiales de datos a los que se refiere

el artículo 9.1. del RGPD, puesto que se trata de datos biométricos dirigidos a la identificación de las personas físicas, es requisito previo que concurra alguna de las circunstancias contempladas en su apartado 2 que levante la prohibición de tratamiento de dichos datos, establecida con carácter general en su apartado 1, exigiendo el artículo 9.2. de la LOPDGDD que “Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.” no existiendo, como se ha indicado, norma legal que habilite dicho tratamiento al amparo del artículo 9.2.g) del RGPD.

Por lo tanto, dicha prohibición únicamente podrá levantarse en aquellos casos en que el afectado preste su consentimiento expreso, al amparo de la letra a) del artículo 9.2. del RGPD, debiendo concurrir todos los demás requisitos para otorgar un consentimiento válido que se recogen en la definición del artículo 4.11 del RGPD: “toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”.

III

Aunque la ausencia de causa que levante la prohibición del tratamiento de categorías especiales de datos determina, por sí sola, la ilicitud del tratamiento propuesto, debe señalarse que tampoco concurre una base jurídica que legitimara el mismo al amparo del artículo 6.1. del RGPD sobre la base del interés público.

El concepto de interés público, o el de interés general, que es más frecuentemente utilizado por nuestro texto constitucional, es un concepto jurídico indeterminado con una doble función: dar cobertura legitimadora a la actuación de la Administración y, por otra parte, constituye una de las formas de limitar las potestades administrativas. De este modo, el interés público que, como señala Parejo Alfonso, tiene una clara función directiva del desarrollo normativo (parlamentario o no) del orden constitucional, actúa como criterio delimitador de la actuación de los poderes públicos, por lo que debe, en primer término, ser identificado por el legislador, al objeto de identificar el ámbito en el que se va a desarrollar la actuación de la Administración, sometida al principio de legalidad y a la que le corresponde servir con objetividad a los intereses generales (artículo 103.CE) y, en todo caso, bajo el control de los tribunales, ya que como recuerda la Sentencia del Tribunal Constitucional de 11 de junio de 1984, “No cabe desconocer que la facultad atribuida por la Constitución al Estado para definir el interés general, concepto abierto e indeterminado

llamado a ser aplicado a las respectivas materias, puede ser controlada, frente a posibles abusos y a posteriori, por este Tribunal…".

En primer término, debe partirse de que la existencia de un interés público, que sin duda existe en el ámbito de la prevención del blanqueo de capitales y la financiación del terrorismo, no legitima cualquier tipo de tratamiento de datos personales, sino que deberá estarse, en primer lugar, a las condiciones que haya podido establecer el legislador, tal como prevé el propio artículo 6 del RGPD, en sus apartados 2 y 3, y el artículo 8 de la Ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales (LOPDGDD) que regula el tratamiento de datos basados en una obligación legal y en una misión realizada en interés público o ejercicios de intereses públicos en su artículo 8, en los siguientes términos:

> "1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.
>
> 2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley."

Por consiguiente, el interés público requiere, en primer lugar, su concreción por parte del legislador, tomando en consideración todos los intereses afectados, al objeto de determinar las restricciones que pueden sufrir los intereses particulares como consecuencia de la presencia de dichos intereses generales, lo que debe hacerse a través de una norma con rango de ley.

En el presente caso, sobre la base del interés público, no resultaría de aplicación la base jurídica del del artículo 6.1.e) del RGPD en la medida en que la Ley 10/2010 no atribuye competencias, que son propias de las Administraciones Públicas, a las entidades financieras como sujetos obligados al cumplimiento de dicha norma.

Por otro lado, del análisis de las justificaciones aportadas por la promotora del proyecto, referida a supuestas suplantaciones de identidad, no puede colegirse que las mismas se refieran específicamente al interés público perseguido por la normativa sobre prevención del blanqueo de capitales y financiación del terrorismo, sino más bien a supuestos de fraude en perjuicio de la propia entidad, respondiendo a un interés privado de la misma, lo que no sería admisible, como recuerda, en otro supuesto de aplicación de sistemas de reconocimiento facial, el Auto 72/2021 de la Sección Novena de la Audiencia Provincial de Barcelona de 15 de febrero de 2021:

> "El nivel de intrusión en la vida privada de los interesados ha de entrar en el ya mencionado juicio de proporcionalidad, que según la normativa exige por lo tanto la expresión del consentimiento explícito de los interesados. Si este consentimiento no se recabase explícitamente y no se recogiese por métodos de prueba como puede ser un soporte escrito, como está siendo el caso en este tratamiento de reconocimiento facial, esto debe subsanarse con el respaldo de otra base de legitimación lo suficientemente fuerte como para llegar a justificarse la necesidad de este tratamiento para obtener los fines deseados, como puede ser el mantenimiento del correcto funcionamiento del negocio y la prevención contra robos, hurtos y situaciones de inseguridad para las trabajadores de la empresa. Esta base de legitimación, asegura Mercadona, a través de su petición, es el "interés público" que se recoge de igual forma como legitimación excepcional en la normativa de protección de datos personales. Sin embargo, esto crea dudas a la hora de interpretar su validez o falta de la misma en este caso, al servir realmente la implantación de esta tecnología de mayor forma a un fin privado de la empresa como sería el garantizar la seguridad de sus instalaciones."

IV

Lo que sí establece la Ley 10/2010, por razones de interés público, son obligaciones a dichos sujetos obligados, siendo la base jurídica aplicable a los mismos no la prevista en la letra e) del artículo 6.1. del RGPD, sino la contemplada en la letra c), tal y como señalaba el Informe de esta Agencia 195/2017:

> *"Como es sabido, la Ley 10/2010 y su Reglamento de desarrollo, aprobado por Real Decreto 304/2014, de 5 de mayo, imponen a los sujetos obligados determinadas medidas de diligencia debida. La enumeración más clara de tales medidas aparece recogida en el artículo 13.1 de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo de 20 de mayo de 2015 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del*

terrorismo, y por la que se modifica el Reglamento (UE) no 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión, cuando establece que:

"Las medidas de diligencia debida con respecto al cliente comprenderán las actuaciones siguientes:

a) la identificación del cliente y la comprobación de su identidad sobre la base de documentos, datos o informaciones obtenidas de fuentes fiables e independientes;

b) la identificación del titular real y la adopción de medidas razonables para comprobar su identidad, de modo que la entidad obligada tenga la seguridad de que sabe quién es el titular real; asimismo, en lo que respecta a las personas jurídicas, fideicomisos, sociedades, fundaciones y estructuras jurídicas similares, la adopción de medidas razonables a fin de comprender la estructura de propiedad y control del cliente;

c) la evaluación y, en su caso, la obtención de información sobre el propósito y la índole prevista de la relación de negocios;

d) la aplicación de medidas de seguimiento continuo de la relación de negocios, en particular mediante el escrutinio de las transacciones efectuadas a lo largo de dicha relación, a fin de garantizar que se ajusten al conocimiento que la entidad obligada tenga del cliente y de su perfil empresarial y de riesgo, incluido, cuando sea necesario, el origen de los fondos, y la adopción de medidas para garantizar que los documentos, datos o informaciones de que se disponga estén actualizados.

Cuando las entidades obligadas adopten las medidas mencionadas en las letras a) y b) del párrafo primero, también verificarán que cualquier persona que diga actuar en nombre del cliente esté autorizada a tal fin e identificarán y comprobarán la identidad de dicha persona."

Las medidas se detallan en el Capítulo II de la Ley 10/2010 y en el Capítulo II de su Reglamento de desarrollo, consistiendo las mismas en la obligación de recabar información de los propios clientes o de terceras fuentes en que dicha información pudiera encontrarse disponible. Dichas obligaciones vienen impuestas de forma claramente imperativa en el texto legal, previéndose específicamente en determinados supuestos la obligación de consultar fuentes disponibles, como sucede en el caso de las personas con relevancia pública (artículo 15). Del mismo modo, el artículo 8 de la Ley se refiere a la aplicación por terceros de estas obligaciones.

De este modo, la legislación de prevención de blanqueo de capitales impone a los sujetos obligados, de forma clara, precisa e incondicional, una serie de obligaciones legales de obtención de información, bien directamente de los clientes, bien de terceros cuando así lo prevé. Ello implicaría que el tratamiento de los datos, así como la cesión de los mismos cuando se refiera a la obtención de la información de dichas fuentes, e incluso la obtención de los datos de otras entidades pertenecientes al mismo Grupo, se encontraría amparada, siempre que resulte proporcional al cumplimiento de las obligaciones legales impuestas, por el artículo 6.1 c) del Reglamento general de protección de datos, que habilita el tratamiento de los mismos cuando sea necesario para el cumplimiento de una obligación legal impuesta al responsable del tratamiento."

Por consiguiente, dichas obligaciones legales deben cumplirse en los términos que la ley que las impone establece que, a los efectos del presente informe, se refiere a la identificación por documentos fehacientes, siendo dicho documento, para los ciudadanos españoles, el Documento Nacional de Identidad, respecto del que el artículo 8 de la Ley orgánica 4/2015, de 30 de marzo, de medidas para la protección de la seguridad ciudadana establece, bajo la rúbrica "Obligaciones y derechos del titular del Documento Nacional de Identidad" lo siguiente:

"1. Los españoles tienen derecho a que se les expida el Documento Nacional de Identidad.

El Documento Nacional de Identidad es un documento público y oficial y tendrá la protección que a estos otorgan las leyes. Es el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular.

2. En el Documento Nacional de Identidad figurarán la fotografía y la firma de su titular, así como los datos personales que se determinen reglamentariamente, que respetarán el derecho a la intimidad de la persona, sin que en ningún caso, puedan ser relativos a la raza, etnia, religión, creencias, opinión, ideología, discapacidad, orientación o identidad sexual, o afiliación política o sindical. La tarjeta soporte del Documento Nacional de Identidad incorporará las medidas de seguridad necesarias para la consecución de condiciones de calidad e inalterabilidad y máximas garantías para impedir su falsificación.

3. El Documento Nacional de Identidad permite a los españoles mayores de edad que gocen de plena capacidad de obrar y a los menores emancipados la identificación electrónica de su titular, así como la firma electrónica de documentos, en los términos previstos en la legislación específica. Las personas con capacidad modificada judicialmente podrán

ejercer esas facultades cuando expresamente lo solicite el interesado y no precise, atendiendo a la resolución judicial que complemente su capacidad, de la representación o asistencia de una institución de protección y apoyo para obligarse o contratar.
El prestador de servicios de certificación procederá a revocar el certificado de firma electrónica a instancia del Ministerio del Interior, tras recibir éste la comunicación del Encargado del Registro Civil de la inscripción de la resolución judicial que determine la necesidad del complemento de la capacidad para obligarse o contratar, del fallecimiento o de la declaración de ausencia o fallecimiento de una persona."

Por lo tanto, 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, tal y como se analizará más adelante.

V

Por último, y sin perjuicio de los señalado anteriormente, deberían respetarse los demás principios del artículo 5 del RGPD, especialmente a los de limitación de la finalidad y minimización de datos.

Especialmente, en relación con el principio de minimización de datos, que requiere que sean "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" (artículo 5.1.c) del RGPD) hay que señalar que en una sociedad altamente bancarizada la propuesta del tratamiento de datos de reconocimiento facial prevista en el proyecto implicará el tratamiento a gran escala de categorías especiales de datos sujetos a un régimen reforzado de garantías. Ello es así por el elevado volumen de clientes de las entidades bancarias que operan en España, así como por cuanto que dicho tratamiento debería generalizarse al conjunto de las entidades financieras u otros sujetos obligados por la Ley PBC/FT.

Además, este tratamiento masivo de datos afectará en su mayor parte a clientes respecto de los que no serán de aplicación las medidas específicas de diligencia previstas en dicha norma, al aplicarse indiscriminadamente a todos los clientes o potenciales clientes independientemente del riesgo existente.

Asimismo, se estaría desconociendo lo dispuesto en el artículo 8 de la Ley Orgánica 4/2015, que como hemos visto, destaca la referencia a que el DNI es el documento público y oficial con suficiente valor por sí solo para la acreditación de la identidad y de los datos personales de su titular, de lo que se desprende que ni siquiera las Fuerzas y Cuerpos de Seguridad del Estado disponen de información de datos identificativos a gran escala basado en datos biométricos de reconocimiento facial contemplada en el proyecto.

Por otro lado, el sistema propuesto no cumpliría con los requisitos de proporcionalidad exigidos por el Tribunal Constitucional, ya que, si bien puede considerarse idóneo para la finalidad propuesta, el mismo no es necesario, al existir medidas alternativas menos intrusivas, ni es estrictamente proporcional, en la medida en que se deriven más beneficios para el interés público que perjuicios sobre otros bienes o valores en conflicto, teniendo en cuenta que se pretende su aplicación masiva e indiscriminada para todos los clientes del sujeto obligado, y que en caso de generalizarse implicaría un tratamiento masivo de categorías especiales de datos que alcanzaría a la práctica totalidad de la población, independientemente del nivel de riesgo que represente desde la perspectiva de la prevención del blanqueo de capitales y la financiación del terrorismo, convirtiéndose la excepción de la posibilidad de tratamiento de datos biométricos en la regla general, en contra de lo pretendido por el RGPD.

Precisamente, la improcedencia de usar estas técnicas con carácter generalizado, se recoge en el ya citado Auto de la Audiencia Provincial de Barcelona:

> “Expuesto lo que precede en los párrafos precedentes, esta Sala considera que la medida peticionada por parte de la entidad, mercantil, MERCADONA S.A, en modo alguno resulta proporcional, necesaria ni asimismo idónea. Los penados en la presente ejecutoria, señores Juan Ignacio Esmeralda se les impuso una prohibición de acceso a un concreto supermercado de la entidad Mercadona, concretamente ubicado en la calle Frederic Mompou s/n de la localidad de San Boi de Llobregat; no se ha tenido constancia, o al menos del testimonio de particulares remitidos a esta sección, no consta que los mismos quebrantasen la correspondiente prohibición de acceso al centro comercial ni asimismo que éstos sean reincidentes en dicha conducta. Pero es más, esta Sala no puede compartir que con la medida interesada se esté protegiendo el interés público, sino más bien, los intereses privados o particulares de la empresa en cuestión, pues como ya se ha explicitado en los párrafos anteriores, se estarían conculcando las garantías adecuadas en orden a la protección de los derechos y libertades de los interesados, no ya sólo de los que han sido penados y cuya prohibición de acceso les incumbe, sino del resto de personas que acceden al citado supermercado”

En consecuencia, la propuesta de tratamiento de datos basados en el reconocimiento facial con fines de identificación en el marco de la ley PBC/FT no está autorizada de acuerdo con el artículo 9.2.g) del RGPD, carece de base de legitimación al amparo del artículo 6.1 del mismo y es contraria a los principios de necesidad, proporcionalidad y minimización.

Siendo, por consiguiente, un tratamiento ilícito, dicha ilicitud no puede obviarse mediante la aplicación de medidas de seguridad proactiva, ya que la ilicitud del tratamiento determina que las mismas sean irrelevantes, por lo que no se procede al análisis de las mismas.

Conforme a lo que se ha expuesto, la Agencia Española de Protección de Datos emite un **informe desfavorable** a la tramitación del proyecto referenciado.