

N/REF: 0097/2020

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente 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, solicitado, con carácter de urgencia, de esta Agencia Española de Protección de Datos de conformidad con lo dispuesto en los artículos 57.1.c) 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD) y 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 428/1993, de 26 de marzo, cúmpleme informarle lo siguiente:

I

Tal y como se señala en su artículo 1, el proyecto de orden remitido “tiene por objeto regular las condiciones y requisitos técnicos mínimos aplicables a la verificación de la identidad y, si procede, otros atributos específicos, de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación distintos a la presencia física que aporten una seguridad equivalente en términos de fiabilidad, de acuerdo con lo previsto en el artículo 7.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y en el artículo 24.1 d) del Reglamento (UE) 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 el que se deroga la Directiva 1999/93/CE”.

Dicha orden se dicta al amparo de lo previsto en el artículo 24.1 del Reglamento (UE) nº 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 el que se deroga la Directiva 1999/93/CE:

Artículo 24

Requisitos para los prestadores cualificados de servicios de confianza

1. Al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios de confianza verificará, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si

procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado.

La información a que se refiere el párrafo primero será verificada por el prestador de servicios de confianza bien directamente o bien por medio de un tercero de conformidad con el Derecho nacional:

- a) en presencia de la persona física o de un representante autorizado de la persona jurídica, o
- b) a distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física o de un representante autorizado de la persona jurídica previamente a la expedición del certificado cualificado, y que cumplan los requisitos establecidos con el artículo 8 con respecto a los niveles de seguridad «sustancial» o «alto», o
- c) por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con la letra a) o b), o
- d) utilizando otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física. La seguridad equivalente será confirmada por un organismo de evaluación de la conformidad.

Asimismo, se fundamenta en la previsión contenida en el apartado 2 del artículo 7 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, que al regular la *Comprobación de la identidad y otras circunstancias de los solicitantes de un certificado cualificado*, dispone lo siguiente:

2. Reglamentariamente, mediante Orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, se determinarán otras condiciones y requisitos técnicos de verificación de la identidad a distancia y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física según su evaluación por un organismo de evaluación de la conformidad. La determinación de dichas condiciones y requisitos técnicos se realizará a partir de los estándares que, en su caso, hayan sido determinados a nivel comunitario.

Serán considerados métodos de identificación reconocidos a escala nacional, a los efectos de lo previsto en el presente apartado, aquellos que aporten una seguridad equivalente en términos de fiabilidad a la presencia física y cuya equivalencia en el nivel de seguridad sea certificada por un organismo de evaluación de la conformidad, de acuerdo con lo previsto en la normativa en materia de servicios electrónicos de confianza.

Por otro lado, como antecedentes de dicha regulación, se manifiesta en el preámbulo que “La emergencia sanitaria generada por la crisis de la COVID-19 ha exigido durante el estado de alarma el confinamiento de la ciudadanía y la drástica limitación de los desplazamientos personales, con vistas a frenar el crecimiento de los contagios. De forma transitoria y excepcional, a través de la disposición adicional undécima del Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente a la COVID-19, se habilitó un sistema temporal de identificación remota para la obtención de certificados cualificados, con el fin de contribuir a reducir los desplazamientos de los ciudadanos para realizar trámites, sin mermar sus derechos”. El texto de la citada disposición, que no fue informada por esta Agencia, es el siguiente.

Disposición adicional undécima. Medidas provisionales para la expedición de certificados electrónicos cualificados.

Durante la vigencia del estado de alarma, decretado por el Real Decreto 463/2020, de 14 de marzo, se permitirá la expedición de certificados electrónicos cualificados de acuerdo con lo previsto en el artículo 24.1.d) del Reglamento (UE) 910/2014, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. A tal efecto, el organismo supervisor aceptará aquellos métodos de identificación por videoconferencia basados en los procedimientos autorizados por el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias o reconocidos para la expedición de certificados cualificados por otro Estado miembro de la Unión Europea. La equivalencia en el nivel de seguridad será certificada por un organismo de evaluación de la conformidad. Los certificados así emitidos serán revocados por el prestador de servicios al finalizar el estado de alarma, y su uso se limitará exclusivamente a las relaciones entre el titular y las Administraciones públicas.

Asimismo, debe citarse como antecedente, aunque no se haga referencia en la documentación remitida, la disposición adicional quinta del Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, que no figuraba en el texto remitido a informe de esta Agencia, y que modificó la Ley de firma electrónica con la misma finalidad pretendida por el artículo 7.2 de la Ley 6/2020, que ha derogado la misma:

Disposición final quinta. Modificación de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Se añade un nuevo apartado 6 al artículo 13 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, con el siguiente tenor:

«6. Por Orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se determinarán las condiciones y requisitos técnicos aplicables a la verificación de la identidad y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física.»

Este texto se corresponde con el que se contenía en el artículo 7.2. del texto del “Anteproyecto de Ley sobre determinados aspectos de los servicios electrónicos de confianza” que fue informado por esta Agencia el 7 de febrero de 2018 (Informe 283/2017), con la única diferencia de la elevación del rango de la disposición que debería aprobarse:

“Por resolución del Secretario de Estado para la Sociedad de la Información y la Agenda Digital se determinarán las condiciones y requisitos aplicables a la verificación de la identidad y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado mediante otros medios de identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física”.

Sin embargo, el texto definitivo de la Ley 6/2020, siguiendo el precedente del Real Decreto Ley 11/2020, procede a identificar algunos de los medios a través de los cuales podrá realizarse dicha identificación, al referirse expresamente a la videoconferencia o vídeo-identificación, convirtiendo de este modo unos sistemas que habían sido admitidos en nuestro ordenamiento jurídico con una finalidad específica dirigida a la prevención del blanqueo de capitales por la autorización de procedimientos de identificación presencial mediante videoconferencia de 12 de febrero de 2016 y la autorización de procedimientos de vídeo-identificación de 11 de mayo de 2017 del Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC), y que se habían establecido con carácter temporal para la expedición de certificados electrónicos cualificados durante la vigencia del estado de alarma declarado como consecuencia de la emergencia sanitaria generada por la crisis de la COVID-19, en medios permanentes admitidos por el ordenamiento jurídico para verificar la identidad a distancia y que no quedarán limitados exclusivamente para los prestadores de servicios electrónicos de confianza, ya que como señala la Memoria de Análisis Normativo (MAIN), “estos productos resultan muy atractivos para otro tipo de empresas que precisen identificar fehacientemente a sus clientes”.

Por otro lado, destaca la ausencia de referencias en el texto remitido a la normativa de protección de datos personales, no obstante la incidencia que la misma tiene en la materia objeto de regulación, en cuanto implica tratamientos automatizados de datos personales que, además, pueden implicar un alto riesgo para los derechos y libertades de los afectados, sin que se considere suficiente, a estos efectos, las referencias puntuales que se contiene en el

artículo 9 respecto a la adopción de “las medidas adecuadas que garanticen la privacidad de todo el proceso de identificación del solicitante”, en el artículo 6 respecto de la formación del operador encargado de la verificación de la identidad en materia de protección de datos personales o en el artículo 8 al referirse al trabajo a distancia.

La necesidad de respetar, en todo caso, la normativa sobre protección de datos personales se recoge expresamente el Reglamento eIDAS, si bien referida a la normativa vigente en el momento de su aprobación, señalando en su Considerando 11 que “El presente Reglamento debe aplicarse de forma que se cumplan plenamente los principios relativos a la protección de los datos personales establecidos en la Directiva 95/46/CE del Parlamento Europeo y del Consejo. A tal efecto, visto el principio de reconocimiento mutuo que establece el presente Reglamento, la autenticación a efectos de un servicio en línea debe implicar exclusivamente el tratamiento de los datos identificativos que sean adecuados, pertinentes y no excesivos para la concesión del acceso al servicio en línea de que se trate. Por otra parte, los prestadores de servicios de confianza y el organismo de supervisión deben respetar asimismo los requisitos de confidencialidad y seguridad del tratamiento previstos en la Directiva 95/46/CE” y estableciendo en su artículo 5.1 que “El tratamiento de los datos personales será conforme a lo dispuesto en la Directiva 95/46/CE” y conteniendo numerosas remisiones a esta normativa a lo largo de su articulado. En este mismo sentido, el artículo 8 de la Ley 6/2020 se refiere a la protección de datos personales:

1. El tratamiento de los datos personales que precisen los prestadores de servicios electrónicos de confianza para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta Ley se sujetará a lo dispuesto en la legislación aplicable en materia de protección de datos de carácter personal.
2. Los prestadores de servicios electrónicos de confianza que consignen un pseudónimo en un certificado electrónico deberán constatar la verdadera identidad del titular del certificado y conservar la documentación que la acredite.
3. Dichos prestadores de servicios de confianza estarán obligados a revelar la citada identidad cuando lo soliciten los órganos judiciales y otras autoridades públicas en el ejercicio de funciones legalmente atribuidas, con sujeción a lo dispuesto en la legislación aplicable en materia de protección de datos personales.

Por consiguiente, siendo dicha normativa de aplicación a los tratamientos de datos personales necesarios para la identificación no presencial de personas físicas para la expedición de certificados electrónicos cualificados que regula la norma objeto de informe, debe de introducirse una

referencia a la observancia de la misma en el preámbulo, así como un artículo específico, proponiéndose la siguiente redacción:

Artículo XX. Protección de datos de carácter personal:

“Los tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y en el resto de la normativa sobre protección de datos personales”.

No obstante, la mera inclusión de dicho precepto no se considera suficiente a los efectos de garantizar adecuadamente el derecho fundamental a la protección de datos de carácter personal, atendiendo al principio de responsabilidad proactiva introducido por el Reglamento general de protección de datos (RGPD) y a la doctrina constitucional relativa a las limitaciones del derecho fundamental a la protección de datos, tal y como se analiza a continuación.

II

En el momento actual, en lo que a la materia de protección de datos personales se refiere, la normativa a la que debe ajustarse el anteproyecto sometido a consulta es el Reglamento (UE) 2016/679, ya citado (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

A este respecto hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”. Dentro de este nuevo sistema, es el responsable del tratamiento el que, a través de los instrumentos regulados en el propio RGPD como el registro de actividades del tratamiento, el análisis de riesgos o la evaluación de impacto en la protección de datos

personales, debe garantizar la protección de dicho derecho mediante el cumplimiento de todos los principios recogidos en el artículo 5.1 del RGPD, documentando adecuadamente todas las decisiones que adopte al objeto de poder demostrarlo.

Asimismo, partiendo de dicho principio de responsabilidad proactiva, dirigido esencialmente al responsable del tratamiento, y al objeto de reforzar la protección de los afectados, el RGPD ha introducido nuevas obligaciones exigibles no sólo al responsable, sino en determinados supuestos, también al encargado del tratamiento, quien podrá ser sancionado en caso de incumplimiento de las mismas.

Por consiguiente, siendo los principales destinatarios de las obligaciones recogidas en el RGPD los responsables y encargados, no obstante, su observancia supone la necesidad de adopción de determinadas conductas por parte del legislador nacional, al objeto de garantizar el cumplimiento del RGPD y, en definitiva, la adopción de garantías suficientes para la protección del derecho fundamental, singularmente cuando se trate de tratamientos de datos personales legitimados como consecuencia del cumplimiento de obligaciones legales o para el cumplimiento de una misión de interés público o el ejercicio de potestades públicas.

A este respecto, debe recordarse, tal y como se indicaba en nuestro Informe 283/2017, que el tratamiento de los datos personales necesario para comprobar la identidad y circunstancias de los solicitantes de los certificados cualificados estará legitimado por el artículo 6.1 c) del Reglamento General de Protección de Datos, que habilita el tratamiento basado en una obligación legal impuesta por el derecho interno o de la Unión Europea.

En estos supuestos, el RGPD contiene previsiones específicas al respecto, comenzando con las previstas en su propio artículo 6, apartados 2 y 3:

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

- a) el Derecho de la Unión, o
- b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra

e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

Asimismo, el artículo 4, después definir en su apartado 7 el «responsable del tratamiento» o «responsable» como “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento” añade que “si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”.

Por otro lado, el artículo 35 regula la evaluación de impacto relativa a la protección de datos (EIPD), señalando que “Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares”. No obstante, dicho precepto prevé que la EIPD haya sido realizada previamente por el legislador en su apartado 10:

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

Por otro lado, debe tenerse igualmente en cuenta que, en el caso de que la obligación venga impuesta por una norma de derecho interno, la misma deberá tener rango de ley, por exigirlo el artículo 53.1 de la Constitución, tal y como expresamente recoge el artículo 8.1 de la LOPDGDD, añadiendo 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” y deberá tenerse en cuenta la doctrina constitucional recogida, fundamentalmente, en las sentencias 292/2000 de 30 noviembre y 76/2019 de 22 de mayo, conforme a la cual los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas, siendo la propia ley la que habrá de contener las garantías adecuadas frente a la recopilación de datos personales que autoriza. El Tribunal Constitucional (TC) ha sido claro en cuanto a que 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 artículo 53.1 CE (...). Es evidente que, si la norma incluyera una remisión para la integración de la ley con las garantías adecuadas establecidas en normas de rango inferior a la ley, sería considerada como una deslegalización que sacrifica la reserva de ley ex artículo 53.1 CE, y, por este solo motivo, debería ser declarada inconstitucional y nula. (...). Se trata, en definitiva, de “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”. Tampoco sirve por ello que para el establecimiento de dichas garantías adecuadas y específicas la ley se remita al propio RGPD o a la LOPDGDD.

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).”

La misma doctrina sostiene el Tribunal de Justicia de la Unión Europea (TJUE). Así, si el art. 8 de la Carta Europea de los Derechos Fundamentales reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, el art. 52.1 reconoce que ese derecho no es ilimitado y permite la limitación del ejercicio de esos derechos y libertades reconocidos por la Carta, limitación que deberá ser establecida por la ley y respetar el contenido esencial de los mismos.

Pues bien, la STJUE de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, (no disponible aún a esta fecha en español), en su apartado 175, recuerda que:

*With regard to the justification for such interference, the requirement, established in Article 52(1) of the Charter, that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits that interference with those rights must **itself** define the scope of the limitation on the exercise of the right concerned (see, to that effect, judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 175 and the case-law cited).*

Igualmente, el apartado 65 de la Sentencia (STJUE) de la misma fecha 6 de octubre de 2020 (C-623/17), Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, con cita, como la anterior, de la sentencia Schrems 2, dice:

*Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir **ella***

***misma** el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).*

En definitiva, el apartado 175 de la STJUE de 16 de julio de 2020, C-311/2020, Schrems 2, dice: *Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir **ella misma** el alcance de la limitación del ejercicio del derecho de que se trate [dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].*

Es pues, la misma ley que establece la injerencia en el derecho fundamental la que ha de determinar las condiciones y garantías, esto es, el alcance y la limitación, que han de observarse en dichos tratamientos,

Y en dicha STJUE de 16 de julio de 2020, Schrems 2, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):

*176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer **reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas**, de modo que las personas cuyos datos se hayan transferido dispongan de **garantías suficientes** que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada].*

La STJUE de 6 de octubre de 2020, en el caso C-623/17, añade la mención de las categorías especiales de datos:

*68 (...) Estas consideraciones son aplicables en particular cuando está en juego la protección de esa **categoría particular de datos personales que son los datos sensibles** [véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55, y de 21 de diciembre de*

2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 117; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 141].

Partiendo de las normas y de la doctrina jurisprudencial citada, esta Agencia viene señalando en sus informes más recientes la necesidad de que, por parte del legislador, al introducir regulaciones en nuestro ordenamiento jurídico que tengan especial trascendencia en los tratamientos de datos de carácter personal, se proceda previamente a un análisis de los riesgos que puedan derivarse de los mismos, incluyendo en la Memoria de Análisis de Impacto Normativo un estudio sistematizado del impacto que en el derecho fundamental a la protección de datos personales de los interesados han de tener los distintos tratamientos de datos que prevé la ley. En este sentido se han pronunciado el Informe 77/2020, relativo al Anteproyecto de Ley Orgánica de Lucha contra el Dopaje en el Deporte o el Informe 74/2020 referido al Anteproyecto de Ley de memoria democrática.

Aplicando dichos criterios al presente caso, **hay que partir de la base de que la norma informada carecería, de acuerdo con la jurisprudencia citada hasta ahora, del rango oportuno para establecer limitaciones al derecho fundamental a la protección de datos**, siendo la regulación contenida en el artículo 7 de la Ley 6/2020 la que ha introducido la posibilidad de que la verificación de la identidad se lleve a cabo mediante otros medios de identificación como videoconferencia o video-identificación, habilitando al desarrollo reglamentario para determinar las condiciones y requisitos técnicos de los mismos, que no podrán afectar al derecho fundamental a la protección de datos. **Por ello, se considera imprescindible, dada la finalidad de la norma objeto de informe, que se analice detalladamente la incidencia que las misma puede tener en los tratamientos de datos personales, al objeto de evitar cualquier extralimitación de la misma que sería determinante de su nulidad.**

Asimismo, pretendiendo la norma que las medidas organizativas y procedimentales que deberán implementar los prestadores sean proporcionadas a los riesgos y adecuadas a las naturaleza de estos servicios respecto de unos certificados que, en palabras de su preámbulo “constituyen un auténtico *alter ego* digital de la persona”, y añadiendo la MAIN, entre sus objetivos específicos, el de “proporcionar a los ciudadanos una alternativa segura desde el punto de vista jurídico y técnico a la personación física para la obtención de certificados cualificados”, y considerando además que tiene efecto positivos sobre la innovación, ya que “permitirá el desarrollo y la puesta en el mercado de soluciones tecnológicas innovadoras, a la vez que seguras”, **el análisis detallado de los riesgos que pueda tener para los derechos y libertades de los ciudadanos permitirá que las medidas que se**

establezcan en la orden respondan, igualmente, a la necesaria seguridad de los datos personales.

Por dichas razones, se considera necesario evaluar el impacto que la regulación contenida tiene en el derecho fundamental a la protección de datos, para garantizar la adecuada protección al derecho fundamental a la protección de datos de los interesados, siendo deseable en estos supuestos una mayor interlocución con esta Agencia, similar a la que se ha mantenido con el Centro Criptológico Nacional, el sector de prestadores de servicios de confianza y de fabricantes de soluciones de identificación a distancia.

III

Analizando ya el texto articulado desde la perspectiva de la protección de datos personales, interesa destacar lo siguiente:

En primer lugar, la licitud del tratamiento de los datos de carácter personal requerirá la existencia de **una base jurídica que legitime el tratamiento**, debiéndose tener en cuenta que el RGPD, a diferencia de lo que ocurría en la normativa anterior, ha situado a todas las bases jurídicas en pie de igualdad, de modo que el consentimiento se recoge como una de las seis causas de legitimación para el tratamiento sin ostentar mayor o menor importancia que las restantes regulando, incluso, supuestos en que el consentimiento del afectado no debe constituir la base legal del tratamiento. Como viene señalando la AEPD desde su informe 65/2017, el RGPD ha desplazado el “principio de consentimiento” como eje central del derecho a la protección de datos, por lo que “ya no puede hablarse de la existencia de excepciones al consentimiento, sino que, siendo el consentimiento una de las posibles bases legítimas del tratamiento no procederá recabarlos en los supuestos en los que el tratamiento se encuentre amparado por cualquiera de las causas restantes causas incluidas en el artículo 6.1 del reglamento general de protección de datos”.

En el presente caso, la base jurídica que legitima el tratamiento, tal y como se ha señalado anteriormente, es la prevista en la letra c) del artículo 6 del RGPD (el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento), por lo que, a estos efectos, no procede recabar el consentimiento del afectado.

No obstante, en el caso de que el posible dato personal a tratar por los prestadores (puesto que habrán de verificar la identidad, o, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, art. 7.2 ley 6/2020) **se trate de alguna de las categorías especiales de datos** a los que se refiere el artículo 9.1. del RGPD será preciso, con carácter previo,

que concurra alguna de las causas que levantan la prohibición de su tratamiento, conforme al artículo 9.2. del RGPD y el artículo 9 de la LOPDGDD. A estos efectos, la orden hace referencia en su artículo 9.8. a la **“comparación biométrica realizada”, lo que podría suponer un tratamiento de datos biométricos dirigido a la identificación unívoca de la persona**. A este respecto, no existiendo norma legal que ampare dicho tratamiento por la existencia de un interés público esencial, con los requisitos y garantías anteriormente señalados, dicho tratamiento únicamente podría basarse en lo previsto en la letra a) del artículo 9.2. del RGPD: “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”, no encontrándose el tratamiento de dichos datos biométricos entre los supuestos en que el artículo 9.1 de la LOPDGDD dispone que el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos. No obstante, el consentimiento deberá cumplir, en todo caso, con los requisitos contenidos en el propio RGPD, que define al consentimiento en su artículo 4.11 como “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”, requiriéndose, además, en este caso, tal y como señala el artículo 9.2.a) que el mismo sea explícito. Asimismo, deberá tenerse en cuenta especialmente, tal y como se indicaba en nuestro informe 36/2020, que el consentimiento debe ser libre, señalando el Considerando 42 del RGPD que “El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno”, por lo que deberán arbitrarse, en todo caso, otras formas de identificación mediante el empleo de otras tecnologías, que no requieran el tratamiento de datos biométricos, al objeto de garantizar la libertad de elección del afectado.

Por todo ello, debería matizarse el artículo 9.2., relativo a las condiciones generales del proceso de identificación, que dispone que “Se recabará el consentimiento expreso del solicitante, incluyendo el consentimiento a la grabación íntegra del proceso de identificación”, ya que **dicho consentimiento, desde la perspectiva de la protección de datos personales, únicamente sería necesario en el caso del tratamiento de categorías especiales de datos personales, debiendo entonces prestarse de manera diferenciada respecto a cualquier otro consentimiento que se estime necesario, conforme al artículo 7.2. del RGPD, y debiendo, asimismo, garantizarse otras formas alternativas de identificación que no supongan dicha injerencia reforzada en el derecho fundamental a la protección de datos personales que supone la grabación y conservación de su imagen y sus datos biométricos**. Y, en el caso de que se pretenda imponer como obligación para la identificación no presencial el

tratamiento de datos biométricos dirigidos a la identificación unívoca de la persona, dicha obligación requeriría su establecimiento por una norma con rango de ley, atendiendo a un interés público esencial, que establezca las garantías oportunas, de acuerdo con el artículo 9.2.g) del RGPD: “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”

IV

En segundo lugar, una vez cumplido los requisitos anteriores, deberán adoptarse todas las medidas oportunas para garantizar el cumplimiento de los principios que se recogen en el artículo 5 del RGPD, además del principio de licitud anteriormente reseñado:

1. Los datos personales serán:

- a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
- b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
- c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
- d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
- e) 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»);
- f) 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 u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

A estos efectos, **deberá incluirse, dentro de la información a la que se refiere el artículo 9 de la orden, en su apartado 1 (“Se informará al solicitante, de manera clara y comprensible, de los términos y condiciones del proceso de identificación remota por video, así como de las recomendaciones de seguridad aplicables”) la prevista en la normativa de protección de datos personales, en los términos señalados en el artículo 13 del RGPD, pudiendo facilitarse dicha información “por capas”, al amparo del artículo 11 de la LOPDGDD.**

Asimismo, debe atenderse especialmente a los **principios de limitación de la finalidad y minimización de datos** como manifestaciones del principio de proporcionalidad, analizando si los datos a tratar son estrictamente los necesarios para la finalidad perseguida y si no existen otras alternativas de tratamientos de datos de carácter personal menos gravosas para el afectado. A estos efectos, debe partirse de que la orden desarrolla el artículo 7.2 de la Ley 6/2020, tal y como señala expresamente en su artículo 1, que se refiere a otros métodos de identificación distintos a la presencia física, entre los que cita la videoconferencia o video-identificación pero sin excluir otros, mientras que la orden se limita exclusivamente a los mismos, **por lo que lo primero que debería valorarse es si no existen, asimismo, otros medios alternativos, que incluso puedan ser menos invasivos, como pudiera ser a través de la comprobación remota de la información contenida en el propio certificado del DNI o la identificación por un tercero de confianza.**

Por otro lado, dentro de las modalidades de la identificación remota por video, el artículo 3 de la orden señala que “El proceso de identificación remota por vídeo se podrá realizar de forma asistida, con la mediación síncrona de un operador, o de forma no asistida, sin necesidad de interacción en línea entre un operador y el solicitante, con revisión posterior de un operador”. **Por tanto, se admite una modalidad no asistida, mucho más invasiva y que va a requerir necesariamente la grabación de las imágenes (tal y como establece con carácter general el artículo 11 de la orden), que requeriría una valoración específica respecto, en primer lugar, la necesidad de dicho tratamiento desde el punto de vista de su proporcionalidad, y en el caso de que se estime necesario el mismo, la adopción de garantías reforzadas desde el punto de vista de la protección de datos personales.**

Asimismo, en virtud del **principio de responsabilidad proactiva**, al regular en el artículo 5 los requisitos generales de seguridad debería incluirse expresamente la necesidad de **realizar el análisis de riesgos para los**

derechos y libertades de las personas físicas que exige el artículo 24 del RGPD, atendiendo a los principios de privacidad por defecto y desde el diseño contemplado en el artículo 25 del RGPD y la necesidad de realizar una EIPD conforme al artículo 35, previendo expresamente que, en medidas a implantar como consecuencia del citado análisis de riesgos prevalecerán sobre cualquier otra. Asimismo, dichas medidas deberán revisarse y actualizarse cuando sea necesario, lo que ocurrirá no solo en el caso de que se produzcan cambios en el sistema, como prevé el artículo 5.1. de la orden, sino en cualquier momento en que se tenga conocimiento de que las mismas no son adecuadas o no son suficientes, como puede ser cuando se tenga conocimiento de vulnerabilidades que puedan dar lugar a brechas de seguridad y para las que no haya solución en ese momento, o por modificaciones en el contexto, los procedimientos organizativos o por los avances tecnológicos. Por esa misma razón, debería hacerse referencia al establecimiento de **auditorías de privacidad y revisión continua de las medidas de privacidad** encaminadas a la mejora continua del cumplimiento normativo en materia de protección de datos y a la implantación de las medidas correctoras necesarias para mejorar la seguridad de los datos personales. Se trata, en definitiva, de adoptar **un modelo de gestión continua del riesgo**, tal y como se avanzaba por esta Agencia en la Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD:

“Ante la constante evolución tecnológica y los procesos de transformación digital que sufren las actividades de tratamiento de los datos personales, es crucial abordar dichos procesos desde un modelo enfocado en la gestión continua del riesgo, definiendo desde el diseño las medidas de control y seguridad necesarias para que el tratamiento nazca respetando los requerimientos de privacidad asociados al nivel de riesgo al que está expuesto y evaluando de forma periódica la efectividad de las medidas de control implantadas”.

Por otro lado, también debería modificarse el apartado 6 del citado artículo 5, al objeto de recoger la **obligación de notificar las brechas de seguridad que afecten a datos personales a esta Agencia sin dilación indebida**, en los términos previstos en el artículo 33 del RGPD.

Asimismo, al regular el artículo 8 los requisitos de las instalaciones, **debe valorarse la posible ubicación de los servidores, en la medida en que pueda suponer la existencia de transferencias internacionales de datos**, lo que requeriría, por lo tanto, que las mismas cumplan con los requisitos establecidos en el Capítulo V del RGPD, teniendo en cuenta las limitaciones que se derivan de la interpretación realizada por el Tribunal de Justicia de la Unión Europea en su reciente sentencia de 16 de julio de 2020 en el asunto C-311/18 (Sentencia Schrems2), que declara contraria a Derecho la

Decisión 2016/1250 de la Comisión europea referida a las transferencias a Estados Unidos (Escudo de Privacidad).

En cuanto a los requisitos para la verificación de la identidad del solicitante y del documento de identidad, su apartado 4 establece las medidas obligatorias que se deben implantar para detectar un posible manipulación de la imagen de video, del documento de identidad o del solicitante, entre las que se encuentra la obligatoriedad de contar el afectado con un dispositivo móvil (debiendo valorarse los riesgos que para sus derechos e intereses supone realizar dicho tratamiento obligatoriamente a través de un dispositivo móvil, adoptándose las garantías oportunas) en el que deberá introducirse un código único, debiendo el prestador comprobar “que el dispositivo móvil al que se remite el código se encuentra en posesión del usuario” añadiendo que “El órgano supervisor podrá poner a disposición de los prestadores una plataforma tecnológica de verificación de la asociación del usuario con el dispositivo móvil”.

El citado precepto plantea una serie de cuestiones desde el punto de vista de la protección de datos personales, además de la reseñada respecto a la incidencia de tener que realizar obligatoriamente el tratamiento a través de un dispositivo móvil, lo que requeriría incluir las vulnerabilidades que introduce el móvil en la gestión del riesgo y la EIPD oportuna: por un lado, al ser potestativa la plataforma, debe valorarse y analizarse de qué otra forma podrá darse cumplimiento a esa obligación de verificación, al objeto de proponer las garantías oportunas. Y por otro, deberá regularse previamente la base de datos que asocia al usuario al dispositivo móvil, debiendo determinarse su base jurídica por una norma con el rango oportuno y de acuerdo con los principios de protección de datos, no conteniendo ni el texto de la orden ni la MAIN mayores referencias respecto de esta plataforma.

Por otro lado, atendiendo al **principio de exactitud de los datos**, al admitir el artículo 10.3 que, por problemas técnicos ajenos al prestador, no pueda realizar la consulta que el mismo establece, pueda continuarse con el proceso de identificación “dejando constancia por escrito de la incidencia”, deberá completarse al objeto de establecer **la obligación de realizar dicha consulta tan pronto como sea posible, antes de proceder a la emisión del certificado.**

V

Por todas las razones expuestas en los apartados anteriores, se considera necesario una revisión del texto remitido al objeto de garantizar el cumplimiento de la normativa de protección de datos personales, valorando todos los riesgos que la aprobación de la norma puede suponer para los derechos y libertades de los afectados, para la plena

efectividad de las previsiones del RGPD y de la LOPDGDD de acuerdo con los criterios jurisprudenciales citados en el presente informe.

A estos efectos, hay que destacar que los tratamientos de datos personales que puedan estar realizándose en la actualidad para la identificación no presencial de personas requieren, de acuerdo con el principio de responsabilidad proactiva, que los respectivos responsables hayan adoptado y documentado todas las medidas necesarias para garantizar el cumplimiento de la normativa de protección de datos personales, a través del oportuno análisis de riesgos, EIPD, etc., identificando las bases jurídicas que legitiman el tratamiento y adoptando todas las garantías necesarias de acuerdo con el principio de protección de datos por defecto y desde el diseño, siendo, por consiguiente todo incumplimiento de dicha normativa de su exclusiva responsabilidad.

Sin embargo, en el momento en que se procede por una norma jurídica a regular dichos tratamientos, los mismos estarán obligados a aplicar dicha norma, por lo que previamente será necesario determinar que la misma es conforme con la normativa de protección de datos personales. Esto tiene especial incidencia si, como en el presente caso, se amparan tratamientos más invasivos, como la identificación de forma no asistida, y se establecen obligaciones de tratamientos específicos, como la obligación de grabar íntegramente y en todo caso el proceso de identificación o, muy especialmente, al afectar a categorías especiales de datos, la obligación de realizar una comparación biométrica, tal y como prevé el artículo 9.8.

Por todo ello, tal y como se apuntaba al principio de este informe, **se considera imprescindible que se proceda a un análisis pormenorizado y detallado de las implicaciones que la aprobación de la norma tiene para los derechos y libertades de los afectados, en los términos previstos en el RGPD y que se han ido apuntando a lo largo del presente informe**, de la forma más completa posible dentro de la urgencia con la que el mismo se ha solicitado, teniendo en cuenta que dicho análisis tiene especial relevancia ya que la presente orden no atiende exclusivamente a la situación temporal derivada de la pandemia del Covid-19, sino que pretende regular estos procesos de identificación de manera permanente, para eliminar, en palabras de su MAIN “la desventaja competitiva -derivada de esta laguna regulatoria- de los prestadores de servicios de confianza establecidos en España con respecto a los prestadores establecidos en otros Estados miembros de la UE”.

Dicho análisis permitirá identificar correctamente todas las medidas y garantías que deben adoptarse y, especialmente, aquellas medidas contempladas en la orden que, por no tener un mero carácter técnico sino regular tratamientos que pueden suponer una injerencia en el derecho fundamental a la protección de datos personales, requerirían de una norma con rango de ley, como son las anteriormente referidas a la grabación

íntegra del proceso de identificación, en todo caso, y al tratamiento de datos biométricos dirigidos a la identificación unívoca de la persona.

Por las razones expuestas, se emite informe desfavorable, pendiente de la subsanación de las observaciones realizadas.