003/2024

I

Como con acierto expone la Memoria de Análisis de Impacto Normativo (MAIN) presentada junto con el Proyecto, la modificación normativa propuesta pretende derogar el anterior Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica, al objeto de actualizar la regulación del proceso de expedición, gestión y desarrollo del Documento Nacional de Identidad (DNI), en sus versiones física y digital, lo que requiere una traducción en el plano normativo, en consonancia con lo determinado por determinados textos legales, como son el Reglamento (UE) 2019/1157 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a ciudadanos de la Unión y a los miembros de sus familias que ejerzan su derecho a la libre circulación, así como a la adaptación del proceso de expedición a la obligación impuesta por la Ley 20/2011, de 21 de julio, del Registro Civil, respecto de la figura del Código Personal, o a la adecuación a las previsiones preceptuadas por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Se trata, en definitiva, de adaptar la normativa de expedición del DNI (de 2005, básicamente) a la evolución legislativa, y ello no sólo a los textos legales citados, sino también, y muy especialmente, dicha adaptación habrá de realizarse igualmente a la nueva regulación derivada de la normativa de protección de datos personales, que en esta materia de *expedición* del DNI se ve particularmente afectada por el RGPD, y la LOPDGDD, ya que dicha expedición del DNI conlleva variados tratamientos de datos personales, incluso de carácter sensible o especiales (datos biométricos -rasgos faciales, huellas dactilares-) que requieren una regulación específica.

II

Por ello esta AEPD cree conveniente comenzar este Informe exponiendo la postura respecto de los tratamientos de datos personales en el ámbito de

una norma jurídica del Tribunal Constitucional y del Tribunal de Justicia de la Unión Europea.

1. La sentencia del Tribunal Constitucional (STC) 76/2019, de 22 de mayo, contiene la doctrina relevante sobre el derecho fundamental a la protección de datos personales, y aborda tanto las características como el contenido que ha de tener la normativa que pretenda establecer una injerencia en ese derecho fundamental.

> *(…) Por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas ora incida directamente sobre su desarrollo (artículo 81.1 CE), ora limite o condicione su ejercicio (artículo 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril, FJ 4).*
>
> *(…) Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal «ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica», esto es, «ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención» (STC 49/1999, FJ 4). En otras palabras, «no sólo excluye apoderamientos a favor de las normas reglamentarias […], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites» (STC 292/2000, FJ 15).*

Y ello porque, en el ámbito de las *categorías especiales* de datos personales,

> (…) *el Reglamento general de protección de datos establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales. En cambio,* ***no establece por sí mismo el régimen jurídico aplicable a los tratamientos de datos personales especiales****, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión. Por ende, tampoco fija las garantías que deben observar los diversos tratamientos posibles de datos sensibles, adecuadas a los riesgos de diversa probabilidad y gravedad que existan en cada caso; tratamientos y categorías especiales de datos que son, o pueden ser, muy diversos entre sí. El reglamento se limita a contemplar la posibilidad de que el legislador de la Unión Europea o el de los Estados miembros, cada uno en su ámbito de competencias, prevean y regulen tales tratamientos, y a indicar las pautas que deben observar en su regulación. Una de esas pautas es que* ***el Derecho del Estado miembro establezca «medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado»***

> ***[artículo 9.2.g) RGPD]*** *y que «se ofrezcan garantías adecuadas» (considerando 56 RGPD). Es patente que ese establecimiento de medidas adecuadas y específicas solo puede ser expreso. Si la norma interna que regula el tratamiento de datos personales relativos a opiniones políticas no prevé esas garantías adecuadas, sino que, todo lo más, se remite implícitamente a las garantías generales contenidas en el Reglamento general de protección de datos, no puede considerarse que haya llevado a cabo la tarea normativa que aquel le exige.*

En consecuencia, y tal y como exige el Tribunal Constitucional, la norma que establezca unas determinadas injerencias en el derecho fundamental a la protección de datos personales de los interesados de categorías sensibles requiere que dicha norma, en primer lugar, sea una norma con rango de ley, o de la Unión Europea, y que, además:

a) especifique el interés público esencial o la causa que justifica el levantamiento de la prohibición de tratamiento que fundamenta la restricción del derecho fundamental (FJ 7 de la STC 76/2019). La ley habrá de explicitar de manera expresa cuál es la causa de entre las previstas en el art. 9.2 RGPD que fundamenta la injerencia al derecho fundamental a la protección de datos personales y por ello el Tribunal Constitucional, con cita de su STC 292/2000, **rechaza** que dicha identificación de los fines legítimos de la restricción pueda realizarse mediante **conceptos genéricos o fórmulas vagas**.

b) en segundo lugar, dicha ley, o norma europea, habrá de regular pormenorizadamente las injerencias al derecho fundamental estableciendo reglas claras sobre el alcance y contenido de los tratamientos de datos que autoriza. Es decir, habrá de establecer cuáles son los **presupuestos y las condiciones** del tratamiento de datos personales relativos a las categorías especiales de datos personales que pueden incluirse en dichos registros mediante reglas claras y precisas (STC 76/2019, FJ 7 b)

c) Y, por último, la propia ley o norma de la UE habrá de contener las garantías adecuadas frente a la recopilación de datos personales que autoriza. El TC ha sido claro en cuanto a que:

> *[l]a 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. (…)

Tampoco sirve que para el establecimiento de dichas garantías adecuadas y específicas se pretenda remitirse al propio RGPD o a la LOPDGDD.

2. 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 (CEDF) reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, y 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, dicha limitación deberá ser establecida por la ley y respetar el contenido esencial de los mismos.

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, en su apartado 175, recuerda que:

En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C 311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

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:

65 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).

III

A continuación, cabe mencionar que esta Agencia viene recomendando repetidamente en sus informes que el prelegislador, en aquellos casos, como el presente, en que los tratamientos puedan tener como base jurídica el art. 6.1.c) o e) del RGPD (esto es, tratamientos cuya base es una obligación legal o una misión de interés público), y venga establecida por el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento y tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, como es el caso de las operaciones de tratamiento impuestas por el proyecto que se informa (la obtención del DNI por las

personas físicas es una obligación impuesta por la ley), haga uso de la posibilidad que establece el art. 35.10 RGPD de modo que sea el propio órgano proponente de la disposición general, en el curso del procedimiento de creación de la norma quien realice una evaluación de impacto relativa a la protección de datos (EIPD) como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica. Dicha EIPD habrá de incorporarse, como permite -casi debería decirse que lo impone, pero en cualquier caso no lo prohíbe- el art. 2.1, letra g), del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Este precepto es, además, suficientemente expresivo de la voluntad del legislador de incluir en la MAIN, dentro del concepto "Otros impactos", el análisis del "impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma".

> *g) Otros impactos: La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma*

Dicho análisis de riesgos o la EIPD no se han llevado a cabo por el órgano proponente del proyecto.

Esta Agencia recuerda, asimismo, que el reiterado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) establece que la política de seguridad del sistema de información deberá examinar y tener en cuenta "los riesgos que se derivan del tratamiento de los datos personales" (art. 12.1.f)), así como que en caso de que los sistemas de información traten datos personales (como es el caso), en todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto en caso de resultar agravadas respecto de las previstas en el citado real decreto (art. 3.3).

En definitiva, esta AEPD recomienda que se lleven a cabo, y se incorporen a la MAIN el análisis de riesgos (art. 24 RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD), en su caso, lo que permitirá, a la vista de ello, al propio prelegislador, determinar no sólo las medidas de seguridad necesarias en los sistemas de información, sino las garantías específicas que se requieran para afrontar los riesgos derivados del tratamiento de los datos que el proyecto de Real Decreto establece (ver art. 35.7.d) RGPD). Al no haber una EIPD en el presente caso, como se

especificará en un epígrafe posterior, no se conocen cuáles son esos riesgos que derivan de los tratamientos de datos personales que establece la norma, por lo que a esta Agencia no se le han ofrecido ni los riesgos ni en consecuencia las posibles medidas y garantías que paliarían esos riesgos

Corresponde, cabe recordar, al responsable del tratamiento, en virtud del principio de responsabilidad proactiva (art. 24.1 RGPD) el establecimiento de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, y que ello habrá de hacerlo “desde el diseño” del tratamiento (art. 25.1 RGPD), integrando las garantías en el tratamiento, y ello aconsejaría que las garantías para minimizar los riesgos, una vez conocidos y ponderados en la EIPD tras el análisis de riesgos, se incorporen a la propia norma.

Por otra parte, el artículo 35.3 RGPD establece que la EIPD se requerirá en particular en el caso de: a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o la c) observación sistemática a gran escala de una zona de acceso público.

En el presente caso, en que la norma regula tratamientos masivos de datos biométricos (categorías especiales de datos, como reconoce expresamente el propio Proyecto) mediante un tratamiento automatizado sobre cuya base se toman decisiones que producen efectos jurídicos para las personas físicas o que les afectan significativamente de modo similar, cabe entender que se da el caso a) y el b) anterior, que se plasma en la Lista publicada por la AEPD “LISTAS DE TIPOS DE TRATAMIENTOS DE DATOS QUE REQUIEREN EVALUACIÓN DE IMPACTO RELATIVA A PROTECCIÓN DE DATOS (art 35.4)”, en su apartado 4: “Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos”, e incluso más específicamente el apartado 5 de dicha Lista. “*Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física*.

IV

1. Comenzando ya con el texto del Proyecto, desde el punto de vista de la normativa de protección de datos personales, cabe describir su contenido, en esencia, diciendo que este establece el procedimiento para la tramitación u obtención del DNI, ya sea en versión física o digital -que son distintas aunque compartan, según el Proyecto, la misma naturaleza jurídica- lo que requiere la recogida y plasmación de los datos personales necesarios para su plasmación en la tarjeta física o en el DNI digital (que se obtiene a partir del primero), y posteriormente dichos datos podrán ser objeto de verificación o el documento ser autenticado a los efectos de la identificación del titular del DNI o del aseguramiento de la veracidad del soporte del DNI.

2. Ahora bien, partiendo de la doctrina ya expuesta del Tribunal Constitucional, nos encontramos con que la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, en su art. 8 y siguientes, contiene la obligación de obtención del DNI por las personas físicas mayores de 14 años, y regula determinados datos que habrán de constar necesariamente en él (fotografía y firma), sin que otros datos puedan referirse a la raza, etnia, religión, creencias, opinión, ideología, discapacidad, orientación o identidad sexual, o afiliación política o sindical. En esta norma la finalidad esencial es la identificación de la persona (art. 8.1) y ello, cabe recordarlo, exclusivamente conlleva la obligación de exhibirlo en los casos en que pueda estar en juego la seguridad pública (art. 9.2 y 16.1 LO 4/2015), esto es, en concreto, a) Cuando existan indicios de que han podido participar en la comisión de una infracción, o b) Cuando, en atención a las circunstancias concurrentes, se considere razonablemente necesario que acrediten su identidad para prevenir la comisión de un delito. Sin embargo, la LO 4/2015 no hace referencia a la posibilidad de tratar o incluir datos biométricos en el DNI

3. Sin embargo, la regulación europea conoce otras posibles finalidades para los documentos de identidad, como es el de hacer posible la libertad de circulación de los ciudadanos europeos dentro de la UE (art. 45 CDFUE y art. 20-21 TUE). Para implementar ese derecho se promulgó la Directiva 2004/38/CE, que establece en su art. 4 la necesidad de que los Estados Miembros expidan o renueven a sus ciudadanos, de acuerdo con su legislación, un documento de identidad o un pasaporte en el que conste su nacionalidad. A su vez, y ante los problemas o complicaciones surgidos de los distintos niveles de seguridad entre los documentos de los diferentes Estados miembros, el Reglamento (UE) 2019/1157 ha venido a reforzar la seguridad de los documentos de identidad de los ciudadanos de la Unión que ejerzan su derecho a la libre circulación. Esta norma ha establecido la necesidad de que, con el fin hacer efectivo ese derecho impidiendo fraudes, los documentos de

identidad de los distintos Estados Miembros tengan características comunes, entre los que cabe destacar a estos efectos y en este momento dos en concreto: se *recogerán* datos biométricos de los interesados (imagen facial y dos impresiones dactilares), y se *incorporarán* estos a un medio de almacenamiento *en el propio documento* de identidad, que es una tarjeta física con una características específicas siguiendo las especificaciones técnicas de un documento de la OACI (9303), para que luego puedan ser *verificadas* dicha tarjeta y datos para comprobar la identidad de la persona. Todos estos, *recogida, incorporación y verificación* constituirían tratamientos de datos personales en el sentido del art. 4.2 RGPD

En opinión de esta AEPD, este instrumento normativo, el Reglamento UE 2019/1157, constituiría pues una causa suficiente para levantar la prohibición del tratamiento de los datos biométricos establecida con carácter general en el art. 9.1 RGPD. La verificación de la identidad de las personas a efectos de la finalidad deseada por la norma de permitir el libre ejercicio de movimientos de los ciudadanos de la Unión sin fraude cabe considerarlo una razón de interés público esencial, establecido por una norma de derecho de la Unión, y proporcional al objetivo perseguido, que respeta en lo esencial el derecho a la protección de datos y que establece medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

4. Pero esas medidas no sólo las establece el Reglamento 2019/1157 sino que en algunas ocasiones se remite a los Estados Miembros para su concreción, lo que estos deberán hacer en la norma que regule el tratamiento, esto es, en nuestro caso, en el Proyecto, y ello, como resulta de la doctrina del Tribunal Constitucional, y del TJUE, estableciendo *reglas claras y precisas*, y no vagas e inconcretas que repitan las características generales derivadas de la protección que establece la legislación de rango superior que intentan implementar.

5. Volviendo a la cuestión del Reglamento 2019/117 como causa que levanta la prohibición, ello lo será respecto de los datos biométricos que, como de manera clara y precisa establece el propio Reglamento, se incorporen a las *tarjetas físicas* en qué consisten los documentos de identidad, pero no para otros supuestos, como sería el caso si la versión digital del DNI que se pretende implantar en el Proyecto contuviera los mismos datos biométricos, y ello porque no parece resultar de la regulación que dicho DNI en su versión digital cumpla las especificaciones técnicas del documento que regula el Reglamento 2019/1157, entre otras cosas porque no tiene formato físico ni alberga en la propia tarjeta (porque no existe tal tarjeta) un sistema de almacenamiento seguro que recojan los datos biométricos (Considerando 22 del Reglamento 2019/1157). Ello supone que el DNI en su versión digital, si contuviese datos biométricos (lo que no resulta claro de la regulación que del mismo se hace en el art. 14 y concordantes del Proyecto) necesitaría de otra

base jurídica de rango legal o de derecho de la UE diferente del propio Reglamento 2019/1157, que no regula dicho supuesto.

6. Ello nos lleva a otra cuestión que surge del propio Reglamento 2019/1157, y es que el Proyecto sometido a informe no establece, como expresamente regula el citado Reglamento 2019/1157, que, si bien los identificadores biométricos deben recogerse y almacenarse en el medio de almacenamiento de los documentos de identidad, sin embargo, los datos biométricos recogidos para la expedición del no deben mantenerse en ningún caso más allá de 90 días tras la fecha de expedición del documento. Superado este periodo, dichos datos biométricos deben ser suprimidos o destruidos inmediatamente (Considerando 22 y art. 10.3 del Reglamento 2019/1157). Esto es, este Reglamento 2019/1157 no establece una base jurídica para crear o mantener bases de datos a nivel nacional para el almacenamiento de datos biométricos en los Estados miembros, ni establece una base jurídica para la creación o el mantenimiento de una base de datos centralizada a nivel de la Unión (Considerando 21). Por ello, este Reglamento no es base jurídica suficiente para la conservación de los datos biométricos obtenidos de los ciudadanos en el proceso de obtención del DNI. Y ello sin perjuicio, como reconocen dichos Considerandos, de que puedan ser objeto de un posible tratamiento ulterior para una finalidad distinta con arreglo al Derecho de la Unión y nacional en materia de protección de datos (Considerando 21 y 22), lo que supone una remisión implícita al art. 6.4 y al art. 23.1 RGPD.

7. El Proyecto prevé específicamente que el DNI, tanto en versión digital como física, servirá al ciudadano para identificarse también electrónicamente y para la firma electrónica de documentos (art. 3 Proyecto). Es decir, incorpora al DNI las características de la identificación electrónica reguladas en el 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 (Reglamento eIDAS) y en la ley La Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Al respecto cabe recordar que el Reglamento UE 2019/1157 específicamente prevé como medida de seguridad, que debería de recogerse también en el Proyecto, que *los Estados miembros deben poder almacenar otros datos en un medio de almacenamiento para los servicios electrónicos u otros fines relacionados con el documento de identidad (…). El tratamiento de esos otros datos, así como su recogida y los fines para los que pueden utilizarse, deben ser autorizados por el Derecho de la Unión o nacional. Todos los datos nacionales deben estar separados física o lógicamente de los datos biométricos contemplados en el presente Reglamento y deben tratarse con arreglo al Reglamento (UE) 2016/679* (Considerando 43). Y, además, en el Considerando 15 del Reglamento UE 2019/1157 se establece que *[e]l presente Reglamento no afecta a la utilización de documentos de identidad y*

documentos de residencia con función de identificación electrónica por parte de los Estados miembros para otros fines, ni afecta a las normas establecidas en el Reglamento (UE) nº 910/2014.

Luego, i) la base jurídica para el tratamiento de los datos personales para la identificación y firma electrónicas no es el Reglamento 2019/1157, sino el Reglamento eIDAS o la ley 6/2020, lo que debería de especificarse en el Proyecto y sobre todo en la MAIN, como luego diremos, y (ii) Dichos datos personales para la identificación y firma electrónica habrán de estar separados física o lógicamente de los datos biométricos almacenados en el documento de identidad.

8. En el art. 7.4 del Proyecto se dice que los documentos necesarios para la obtención del DNI serán recabados electrónicamente, salvo que la persona interesada se opusiera a ello *o cuando de manera excepcional, no se pudiera llevar a cabo por falta de medios electrónicos o interrupción de los mismos.* En ambos casos, la persona interesada deberá aportar dichos documentos en formato papel (…). No parece que una norma reglamentaria pueda establecer una excepción, no prevista legalmente, imponiendo una obligación al ciudadano contraria en principio al régimen general establecido en el art. 28.2 ley 39/2015 por defectos achacables al sistema informático de la propia Administración.

En el art. 7.6 del Proyecto se menciona que en la tramitación se recogerán las impresiones dactilares de los dedos índices de ambas manos a la persona interesada. Pero no se menciona dónde se plasmarán los datos biométricos resultantes de dicha actividad de recogida de datos. En el Reglamento 2019/1157 se especifica claramente que dichos datos, junto con la imagen facial se almacenarán en el medio de almacenamiento de los documentos de identidad (art. 3.5 y 11.6), que, dado que es un Reglamento europeo, es de obligado cumplimiento para los Estados miembros, y el Proyecto no dice nada al respecto.

Del mismo modo, el Reglamento 2019/1157, art. 3.6, establece que “los datos almacenados [en dicho dispositivo de almacenamiento obligatorio] serán accesibles en formato sin contacto y seguro, de conformidad con lo dispuesto en la Decisión C(2018) 7767”, y a mayor abundamiento, igualmente con carácter obligatorio, determina que *“[d]ebe ponerse en conocimiento de los interesados la existencia en sus documentos del medio de almacenamiento que contiene sus datos biométricos, incluida su accesibilidad en formato sin contacto, así como de todos los casos en que se utilicen los datos contenidos en sus documentos de identidad (…*)” (Considerando 40). Se trata por tanto de una medida, de información, que se sugiere que se incluya en el Proyecto, a fin de dar cumplido conocimiento a los interesados.

9. En el art. 13, referido al contenido del DNI se enumeran una serie de datos personales que habrán de tratarse, y plasmarse en el DNI. No existe una Evaluación de Impacto que determine si el tratamiento de dichos datos es proporcionado a la finalidad del tratamiento. No significa esto que esta AEPD tenga una opinión contraria a su reflejo en la tarjeta del DNI, entre otras cosas porque los datos que han de figurar vienen establecidos, como de manera genérica en el art. 3.1 Reglamento 2019/1157, con remisión al documento 9303 de la OACI, sino porque no existe una evaluación en la MAIN acerca de la incidencia de estos datos en concreto en el derecho fundamental a la protección de datos de los interesados. Entre estos datos no se mencionan, como ya hemos expuesto, los datos biométricos que sin embargo sí han de incluirse en el medio de almacenamiento de alta seguridad (art. 3.5 Reglamento 2019/1157) que a su vez ha de incluirse en la tarjeta, y ello, también ya mencionado, de manera separada física o lógicamente, de los datos de para servicios o identificación electrónica si se incluyen el mismo DNI, como sería el caso (art. 3.10 Reglamento 2019/1157).

V

El Capítulo IV del Proyecto lleva por título “Sobre las especificidades de la versión digital del Documento Nacional de Identidad”, y contienes tres artículos, arts. 14 a 16, titulados respectivamente Versión digital del Documento Nacional de Identidad, “Certificados electrónicos cualificados” y “Tratamiento de los datos de identidad”. En consecuencia, todos estos artículos deberían de regular diversos aspectos de la versión digital del DNI. Pero no es así exactamente.

Sólo el primero (art. 14) está dedicado a las especificidades de la versión digital del DNI y su regulación es, en cualquier caso, incompleta y además no es la propia de una redacción de una norma jurídica, esto es, clara y específica, sino que más bien parece dirigida a proclamar las bondades desde un punto de vista de una exposición de motivos y no del texto articulado o regulatorio, de la versión digital del DNI sin contener propiamente una regulación (así, apartado 2 del art. 14: *La versión digital del Documento Nacional de Identidad, es complementaria a las características electrónicas que contiene el soporte físico del documento, con la finalidad de aumentar su uso y funcionalidades, sin detrimento de los mecanismos de seguridad en su interacción),* esto es, sin regular específicamente los datos personales que se tratarán de manera diferenciada del DNI en su versión física (si es que efectivamente se tratasen datos diferentes de los anteriores, que no se expresa), las finalidades del tratamiento específicas para la versión digital diferentes de las de la versión física, o una verdadera regulación del procedimiento para su obtención o registro, con las medidas de seguridad pertinentes (expresándose, sin

embargo, en dicho precepto generalidades como que "*se empleará la más avanzada criptografía y diferentes verificaciones biométricas*") y remitiéndose a una norma posterior, de ínfimo rango (probablemente una resolución o Instrucción de la Dirección General de la Policía, a tenor de la redacción del apartado 6 del precepto).

Como ya mencionamos en el epígrafe IV, apartado 5, de este Informe, no queda claro del texto del Proyecto cuál es el contenido efectivo del DNI en su versión digital, o más en concreto si contiene datos biométricos, o si más bien se trata de algún tipo de aplicación que generará algún tipo de respuesta a solicitud del interesado (por ejemplo, un código tipo QR) mediante su conexión con una base de datos central (cuya base jurídica, en su caso, para el tratamiento de los datos, se desconoce) etc. Más bien parece que esta funcionalidad, que es además voluntaria para el interesado (que no significa que el tratamiento pueda tener como base jurídica el consentimiento del interesado, vid Considerando 42 RGPD) va destinada a que el ciudadano pueda decidir, ante determinadas situaciones en las que quizás no sea necesario mostrar todas las características del DNI en su versión física, que sólo se muestren mediante el uso de la versión digital determinados datos de entre todos los que tiene el DNI físico. Esta podría ser la explicación de la redacción del art. 2.3 del Proyecto, cuando dice que: *La versión digital permite a la ciudadanía tener acceso a sus datos personales, usarlos y gestionarlos de forma segura, independientemente de su ubicación;* o del art. 14.3 del Proyecto: *La versión digital del Documento Nacional de Identidad, es complementaria a las características electrónicas que contiene el soporte físico del documento, con la finalidad de aumentar su uso y funcionalidades, sin detrimento de los mecanismos de seguridad en su interacción.* Si así fuera, esta AEPD considerar muy favorable la propuesta por cuanto cumpliría con el principio fundamental de la protección de datos, de la minimización de datos (art. 5.1.c) RGPD), por cuanto los datos personales han de ser siempre los "*limitados a lo necesario en relación con los fines para los que son tratados*".

Ello nos lleva por otra parte a la doble mención que se realiza en el texto del Proyecto a la eficacia de las versiones digital y física del DNI. En el art. 2.3 se dice que ambas versiones tienen la misma "naturaleza jurídica", y en el art. 14.3 que ambas tienen la misma "eficacia jurídica". Ambos conceptos no son idénticos, y el redactor habrá de determinar si ambas versiones "son" lo mismo o si ambas surten los mismos efectos. Pero ello no podría determinarse con la redacción actual del Proyecto porque, en opinión de este Informe, la regulación del Proyecto, en su art. 14, es tan parca e incompleta que no puede determinarse, sobre todo por no conocerse del texto, para el lector de la norma, si la versión digital tiene los mismos atributos (incluidos los datos biométricos) y por lo tanto puede realizarse con dicha versión digital todos, absolutamente todos, los actos jurídicos que permite el documento de identidad en su versión física, y no sólo algunos. Así, por ejemplo, el legislador en el Proyecto no determina si con la versión digital podrían hacerse uso de las libertades de

circulación dentro de la Unión de suerte que se trata (la versión digital) de un mecanismo que ha de ser necesariamente aceptado por los diferentes Estados miembros para entrar en ellos (así, por ejemplo, ¿serviría el DNI versión digital a todos los efectos previstos en el Reglamento UE 23019/1157 o la Directiva 2004/38/CE?), o si esa autoproclamada similar naturaleza/eficacia jurídica lo es a efectos meramente internos, o incluso sólo para algunos casos y las Fuerzas y Cuerpos de Seguridad no podrían, por ejemplo, solicitar el DNI físico si alguien le mostrara exclusivamente la versión digital ante su requerimiento -ya que ambos tendrían los mismo efectos-, lo que no queda claro del Proyecto, y necesitaría de una reflexión por el redactor y su plasmación, en su caso, en el texto de la norma para una mejor comprensión de esta y para la regulación que se pretende.

VI

En cuanto al art. 15, relativo a los certificados electrónicos cualificados, aunque se incluye en el Capítulo IV, sobre la versión digital, en realidad no regula exclusivamente estos en la citada versión digital, sino que los regula para ambos casos (apartados 1 y 2 del artículo). Por eso se considera que este artículo debería de formar parte, como el artículo 16 a continuación, no del Capítulo IV, sino de un capítulo de Disposiciones comunes.

VII

El artículo 16 lleva por título “Tratamiento de datos de identidad”.

Como comentario general esta AEPD sugiere que se revise íntegramente la redacción de este artículo y se redacte conforme a otras normas de superior rango, con una estructura más acorde al objetivo buscado de protección de los derechos e intereses de los ciudadanos, los cuales tienen derecho, como ya hemos ciado al Tribunal Constitucional, a reglas *claras y precisas* acerca de cómo se van a tratar sus datos, y las medidas y salvaguardias establecidas por el legislador a la hora de establecer la necesidad y proporcionalidad del tratamiento. El art. 6.3 RGPD proporciona una referencia o guía, estructurada, de los aspectos que la norma que regule el tratamiento puede contemplar cuando la base jurídica sea una obligación legal o una misión de interés público. Así:

> *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.

Como ejemplo práctico, entre otros, pero aplicable especialmente a este caso ya que igualmente se tratan datos de categoría especial, podemos sugerir la Disposición Adicional Cuarta de la ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte.

Entrando ya en el contenido del art. 16 del Proyecto, esta Agencia sugeriría que se modificase la denominación del precepto para que fuese más genérica, Protección de datos personales, pues ha de hacer referencia a todos los datos personales que pudieran ser tratados en las actividades de tratamiento, ya que algunos no son “datos de identidad” -sin perjuicio de que no hay una definición en la normativa de protección de datos para este concepto específico- (por ejemplo, el dato del domicilio -ver art. 13 Proyecto- sería dato personal pero no “de identidad”).

Además, debería de establecerse este artículo en un capítulo propio, o incluirlo en uno de Disposiciones comunes, o similar, como ha hecho por ejemplo el art. 10 del Reglamento UE 2019/1157, que ha separado en el art. 10 y en el art. 11 materias que en este art. 16 del Proyecto van en el mismo precepto, sin un aparente orden o estructura determinada.

Ello nos lleva a que el apartado 2 del art. 5, que parece hacer referencia a la Dirección General de la Policía como “responsable del tratamiento” se integre en un artículo único, ya que es el “responsable del tratamiento” que se realicen ante cuando se expide o se verifica el DNI físico como el digital.

Volviendo al art. 16, el apartado 1 identifica como bases jurídicas de los tratamientos previstos en la norma la misión de interés público y el interés legal (arts. 6.1.c) y 6.1.e) RGPD), pero no mencionan cuál es la norma con rango de ley o de la UE (véase art. 8 LOPDGDD) que para cada caso justifica dichos tratamientos.

En el apartado 2 debe dejarse claro (porque se hace difícil de comprender la redacción) que es la DGP, en sí misma, la que es "responsable del tratamiento", no alguien dentro de su organización. Así se establece en el art. 11.2 del Reglamento UE 2019/1157:

> *A efectos del presente Reglamento, las autoridades responsables de expedir documentos de identidad y documentos de residencia se considerarán como el responsable a tenor del artículo 4, punto 7, del Reglamento (UE) 2016/679 y serán responsables del tratamiento de los datos personales.*

Ciertamente, esa labora la realizan personas dentro de la estructura orgánica correspondiente, pero la condición de responsable del tratamiento recae en la DGP (no, para que no haya dudas, en su Director/a personalmente).

No se acaba de entender, como ya se ha mencionado, el resto del apartado: no se sabe a qué se hace referencia con "verificación, análisis y auditorías de las consultas que sean necesarias", y para qué, o cual es la función que lleva a cabo el responsable del tratamiento al mencionar aquí específicamente en este apartado esas funciones de verificación de datos especiales.

En el apartado 4 el texto alega como causa que levanta la prohibición del tratamiento de datos personales de carácter especial (entre ellos los biométricos) al art. 9.2.g) RGPS, esto es, cuando el tratamiento es necesario por razones de un interés público esencial, pero ello ha de ser, como continúa dicho artículo, *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;* A este respecto, es de notar que, conforme al art. 9.2, primer párrafo, de la LOPDGDD, dicha norma, si es de derecho español, ha de tener rango de ley, por lo que este Real Decreto (Proyecto), en sí mismo, no es la base a que se refiere el art. 9.2.g) RGPD, por lo que debería de identificar la base jurídica de la que proviene.

VIII

Siguiendo ahora a lo expuesto en el epígrafe III de este Informe, a pesar de la importancia para los interesados y los riesgos que conlleva el tratamiento de datos de salud para el derecho fundamental a la protección de datos, no existe en la MAIN un Análisis de Riegos, y como consecuencia de la no

existencia de dicho Análisis, tampoco parece existir, porque no se menciona, una Evaluación de Impacto en Protección de Datos (EIPD) de la que puedan resultar los riesgos derivados de los tratamientos previsto en la norma y las medidas que puedan mitigar estos, para que los tratamientos de datos personales que resultan no interfieran más allá de lo estrictamente necesario en el derecho fundamental a la protección de datos de que disfrutan las personas físicas.

Desde un punto de vista práctico, esta Agencia ha publicado (abril 2023) sus "Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo" [1], que tiene como objeto servir de guía para la realización de una evaluación de impacto para la protección de datos (EIPD) en el marco de la elaboración de la Memoria de Análisis de Impacto Normativo (MAIN), cuando las iniciativas legislativas de las Administraciones Públicas implican el tratamiento de datos personales. Este documento está orientado a los organismos de las Administraciones Públicas que promuevan proyectos normativos que impliquen tratamientos de datos personales a los que sea de aplicación el RGPD, así como la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (L.O. 7/2021). Asimismo, está dirigido a los Delegados de Protección de Datos (DPD) de los citados organismos con el fin de contribuir al desempeño de sus funciones de asesoramiento en relación con dichos proyectos normativos.

En esta "Guía" se contienen, con profundidad y rigor, los pasos o el método a seguir para determinar la necesidad y el contenido de la Evaluación de Impacto, y entre ellos esta AEPD desea resaltar en este momento el apartado D del epígrafe II del mismo, relativo a las características de la norma que ampara el tratamiento:

> *Toda medida legislativa que habilite un tratamiento debe cumplir con la premisa de "previsto en la ley". Esto implica que debe ser clara y precisa, y su aplicación accesible y previsible para sus destinatarios, de conformidad con el TEDH, el TJUE y el Tribunal Constitucional (TC). Por lo tanto, en la norma han de estar claramente definidos, con precisión y apropiadamente:*
>
> *1.- La finalidad o finalidades del tratamiento.*
>
> *2.- La legitimidad del tratamiento.*
>
> *3.- La descripción de la implementación del tratamiento en sus aspectos relevantes, como pueden las operaciones y los procedimientos*

[1] https://www.aepd.es/es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf

determinantes del tratamiento (por ejemplo, recogida, almacenamiento, acceso, transmisión, difusión,…), las tecnologías planteadas para implementar las operaciones (inteligencia artificial, almacenamiento en Nube, biometría, IoT, móviles, videovigilancia,…), la existencia de decisiones automatizadas, así como la participación o posible participación de encargados y/o subencargados en distintas operaciones del tratamiento, entre otros.

4.- El ámbito y extensión del tratamiento con relación a las categorías de datos personales tratados (especialmente si son categorías especiales), las categorías de interesados afectados, las circunstancias en las que se utiliza la información personal (por ejemplo: de forma sistemática, solo en determinados casos, durante un periodo de tiempo limitado, etc.), los plazos de conservación de los datos, la frecuencia de recogida de datos, la granularidad de los datos y otros factores que definan el alcance del tratamiento.

5.- Los responsables/corresponsables o categorías de responsables y, en su caso, los encargados o categorías de encargos y/o de subencargados.

6.- Las entidades que acceden y a las que se pueden comunicar datos personales, así como los fines de tal comunicación, en particular, las condiciones de la comunicación de datos entre autoridades públicas en virtud de una obligación legal para el ejercicio de una misión oficial según las condiciones del RGPD (Cons. 31):

- *En el marco de una investigación concreta.*
- *De interés general.*
- *De conformidad con el Derecho de la Unión o de los Estados miembros.*
- *Por escrito y de forma motivada.*
- *Con carácter ocasional.*
- *No deben referirse a la totalidad de un fichero.*
- *No deben dar lugar a la interconexión de varios ficheros.*

7.- La justificación de la solución adoptada para el acceso a datos personales, teniendo en cuenta que supone la utilización de datos de conformidad con unos requisitos específicos de carácter técnico, jurídico u organizativo, sin que ello implique necesariamente la transmisión o la descarga de los datos.

8.- Las medidas para garantizar un tratamiento lícito y equitativo, habida cuenta de la naturaleza, alcance (especialmente con relación a las

categorías especiales de datos), contexto y finalidades del tratamiento o de las categorías de tratamientos, los mecanismos de información y transparencia, así como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX del RGPD, en particular, aquella orientadas a evitar los accesos o las transferencias de datos ilícitos o abusivos.

9.- En el caso de limitación por ley de derechos u obligaciones al amparo de los arts. 23 del RGPD o 24 de la L.O. 7/2021, debe estar muy clara su determinación, las condiciones específicas de limitación de las obligaciones y derechos (Cons. 19 del RGPD), y los perjuicios concretos a la consecución de los fines que justifican la falta de información a los interesados sobre la limitación. La lista anterior no es exhaustiva, sino que cualquier otra disposición pertinente, para cada caso concreto, debería incluirse en la descripción del tratamiento.

La MAIN presentada es una Memoria Abreviada. En la Justificación (apartado I) de la Memoria se dice que ello es "*Puesto que de esta propuesta normativa no se derivan impactos apreciables en los ámbitos que se señalan, esta Memoria Abreviada se emite de acuerdo con lo establecido en el artículo 3 del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo".*

Esta Agencia discrepa respetuosamente de dicha conclusión y considera que el Proyecto tiene una incidencia muy importante en el derecho fundamental a la protección de datos personales, ya que basta comprobar que el propio Proyecto reconoce que se tratarán datos biométricos, esto es, de categoría especial (imagen facial y dos huellas dactilares). Por ello se debería de tramitar una Memoria ordinaria, y en ella, aparte de cualesquiera otros contenidos, debería de procederse a un análisis de riesgos y a una Evaluación de Impacto en Materia de protección de datos (EIPD) que permita evaluar la incidencia de la regulación propuesta en el derecho fundamental concernido a la protección de datos personales y que permita evaluar igualmente las medidas necesarias, meramente apuntadas pero no establecidas o analizadas de manera concreta en el texto del proyecto más allá de un buen deseo y la expresión de la necesidad de establecer dichas medidas, pero sin establecer cuales habrán de ser.