

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en la Exposición de Motivos de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos.

El texto remitido tiene por objeto la transposición sin dilación de directivas de índole penal para afrontar procedimientos de infracción abiertos por la Comisión europea, bien como consecuencia del vencimiento del plazo, bien por la necesidad de una más adecuada adaptación, lo que implica introducir las oportunas modificaciones en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal y en la Ley Orgánica 7/2014, de 12 de noviembre, sobre intercambio de información de antecedentes penales y consideración de resoluciones judiciales penales en la Unión Europea, siendo esta última norma la que plantea la principales consideraciones en relación con el tratamiento de datos personales de personas físicas.

I

Tal y como se ha indicado, las principales cuestiones en materia de protección de datos personales de las personas físicas se plantean en las modificaciones introducidas en la Ley Orgánica 7/2014, de 12 de noviembre, sobre intercambio de información de antecedentes penales y consideración de resoluciones judiciales penales en la Unión Europea, por lo que el presente informe se centrará en el análisis de las mismas.

Tal y como se señala en el texto del anteproyecto y en la Memoria de análisis de impacto normativo (MAIN), dichas modificaciones responden a una triple finalidad:

- Transponer a nuestro ordenamiento jurídico la Directiva (UE) 2019/884 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por la que se modifica la Decisión Marco 2009/315/JAI del Consejo en lo que respecta al intercambio de información sobre nacionales de terceros países y al Sistema Europeo de Información de Antecedentes Penales (ECRIS) y por la que se sustituye la Decisión 2009/316/JAI del Consejo.

- Adaptar sus previsiones al Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo de 17 de abril de 2019 por el que se establece un sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas (ECRIS-TCN) a fin de complementar el Sistema Europeo de Información de Antecedentes Penales, y por el que se modifica el Reglamento (UE) 2018/1726.
- Reformar determinados aspectos relativos al intercambio de información de antecedentes penales con el resto de países de la UE que venían siendo regulados tanto en la actual Ley Orgánica 7/2014 como en el RD 95/2009, de 6 de febrero, por el que se regula el Sistema integrado de registros administrativos de apoyo a la Administración de Justicia.

Partiendo de esta triple finalidad, y dada la urgencia con la que se solicita la emisión del presente informe, el mismo se va a centrar en las modificaciones que se introducen en el articulado de la Ley Orgánica 7/2014 y que, a juicio de esta Agencia, no se corresponden adecuadamente con las previsiones previstas en la normativa sobre protección de datos personales, comenzando con la indebida extensión que se realiza de la previsión de incorporar la “imagen facial” entre los datos del condenado a cualquier otro dato biométrico obtenido y conservado conforme al Derecho español.

A este respecto, debemos partir de la diferencia existente entre “imagen facial” y dato biométrico, así como en la consideración del dato biométrico como categoría especial de datos, al tratarse de conceptos diferentes, tal y como se razonaba en nuestro informe 36/2020, referido al empleo de técnicas de reconocimiento facial:

En el presente caso, versando la consulta sobre técnicas de reconocimiento facial dirigidas a acreditar la identidad del alumno, nos encontraríamos ante el tratamiento de datos biométricos, tal y como los define el artículo 4.14 del RGPD:

«datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

No obstante, hay que adelantar que el RGPD no parece considerar a todo tratamiento de datos biométricos como tratamiento de

categorías especiales de datos, ya que el artículo 9.1. se refiere a los “datos biométricos dirigidos a identificar de manera unívoca a una persona física”, por lo que, de una interpretación conjunta de ambos preceptos parece dar a entender que los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física. En este sentido, parece que igualmente se pronuncia el Considerando 51 al señalar que “El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física”.

Con igual criterio, el Protocolo de enmienda al Convenio para la Protección de Individuos con respecto al procesamiento de datos personales, aprobada por el Comité de Ministros en su 128º período de sesiones en Elsinore el 18 de mayo de 2018 (Convenio 108+) incluye únicamente como categorías especiales de datos, en su artículo 6.1 a los datos biométricos dirigidos a la identificación unívoca de una persona (“biometric data uniquely identifying a person”), sin incluir la referencia a la autenticación.

Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía el Grupo del Artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas:

Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).

Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

Esta misma diferenciación se recoge en el Libro blanco sobre la inteligencia artificial de la Comisión Europea:

“En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos”.

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

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

Por consiguiente, la “imagen facial”, en cuanto mera imagen que no ha sido sometida a tratamiento técnico, no puede considerarse, por sí sola, como dato biométrico, en tanto en cuanto no se someta a un tratamiento técnico específico que permita obtener datos relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona.

Esta distinción se recoge específicamente en el Reglamento (UE) 2019/816 que en su artículo 3, apartado 13, define la «imagen facial» como una “imagen digital del rostro de una persona” y la regula en el artículo 6 diferenciando entre el uso de la imagen facial para confirmar la identidad de un

nacional de un tercer país y el empleo de técnicas de reconocimiento facial, que condiciona en su apartado 2 en los siguientes términos:

Artículo 6

Imágenes faciales

1. Hasta la entrada en vigor del acto delegado previsto en el apartado 2, las imágenes faciales solo podrán utilizarse para confirmar la identidad de un nacional de un tercer país que haya sido identificado como consecuencia de una consulta alfanumérica o de una búsqueda con datos dactiloscópicos.

2. La Comisión está facultada para adoptar actos delegados de conformidad con lo dispuesto en el artículo 37, que complementen el presente Reglamento, relativos al uso de imágenes faciales para identificar a los nacionales de terceros países, con el fin de identificar a los Estados miembros que posean información sobre condenas anteriores relativas a dichas personas, cuando sea técnicamente posible. Antes de ejercer dicha facultad, la Comisión, teniendo en cuenta la necesidad y proporcionalidad así como la evolución técnica en materia de instrumentos informáticos de reconocimiento facial, evaluará la disponibilidad y grado de preparación de la tecnología requerida.

Este precepto debe ponerse en relación con el Considerando 24, que incluye entre las consideraciones a tener en cuenta por parte de la Comisión, además de las de carácter técnico, las de naturaleza política:

Inicialmente, las imágenes faciales incluidas en el ECRIS-TCN solo deben utilizarse para confirmar la identidad de un nacional de un tercer país a fin de identificar a los Estados miembros que poseen información sobre condenas anteriores de dicho nacional de un tercer país. En el futuro, debe ser posible utilizar las imágenes faciales para el sistema automatizado de correspondencias biométricas, siempre que se hayan alcanzado las condiciones técnicas y políticas para ello. La Comisión, teniendo en cuenta la necesidad y la proporcionalidad, así como los avances técnicos en el ámbito de los programas informáticos de reconocimiento facial, debe evaluar la disponibilidad y la preparación de la tecnología requerida antes de adoptar el acto delegado relativo a la utilización de imágenes faciales para identificar a los nacionales de terceros países, a fin de identificar a los Estados miembros que poseen información sobre condenas anteriores relativas a dichas personas.

Por su parte, la Directiva (UE) 2019/884 modifica la Decisión Marco 2008/315/JAI para incluir entre la información objeto de transmisión a la que se refiere su artículo 11 la “imagen facial”, que se define, asimismo, como “una imagen digital del rostro de una persona”, sin incluir referencia alguna al reconocimiento facial o a otros datos biométricos, teniendo en cuenta que la Decisión ya incluye entre la información a transmitir las “impresiones dactilares obtenidas del condenado”.

Por otro lado, el Reglamento (UE) 2019/816 reconoce expresamente la importancia de los datos biométricos en su Considerando 25:

La utilización de datos biométricos es necesaria, ya que es el método más fiable tanto para la identificación de nacionales de terceros países en el territorio de los Estados miembros, que con frecuencia no están en posesión de documentos o cualquier otro medio de identificación, como para una correspondencia más fiable de los datos de los nacionales de terceros países.

Y, consecuentemente, el Considerando 26 se refiere a la importancia de los datos dactiloscópicos, a los que dedica una parte importante de su regulación:

La utilización de datos biométricos es necesaria, ya que es el método más fiable tanto para la identificación de nacionales de terceros países en el territorio de los Estados miembros, que con frecuencia no están en posesión de documentos o cualquier otro medio de identificación, como para una correspondencia más fiable de los datos de los nacionales de terceros países.

Y, en lógica concordancia con lo anterior, al definir los datos de identidad en su artículo 3.10, se refiere exclusivamente, además de a los datos alfanuméricos, a “los datos dactiloscópicos y las imágenes faciales utilizadas para establecer una conexión entre tales datos y una persona física”.

Por lo tanto, teniendo en cuenta que la modificación responde a la necesidad de transponer a nuestro ordenamiento jurídico la Directiva (UE) 2019/884 y adecuar nuestra normativa al régimen contenido en el Reglamento (UE) 2019/816, no conteniendo dichas disposiciones comunitarias referencia alguna al tratamiento de otros datos biométricos, debe suprimirse la referencia que a dichos datos se contienen en los siguientes apartados:

Apartado cinco, que modifica en apartado 2 del artículo 7 de la Ley Orgánica 7/2014:

«2. El Registro Central de Penados podrá, además, proporcionar información relativa a impresiones dactilares u otros datos biométricos obtenidos y conservados conforme al Derecho español, así como cualquier otra relativa a la condena que constase en el mismo.»

Apartado seis, que introduce un nuevo artículo 7 bis en la Ley Orgánica 7/2014, cuyo apartado 3 prevé lo siguiente:

3. Cuando el Derecho español permita la recogida y conservación de las imágenes faciales u otros datos biométricos del condenado, podrá remitirse dicha información al Sistema Centralizado, respecto de nacionales de terceros países o apátridas condenados en España.»

Todo ello sin perjuicio de que el tratamiento de otros datos biométricos pueda plantearse en términos de legislación nacional, teniendo en cuenta el criterio restrictivo que respecto del tratamiento de esta categoría de datos mantiene, en consonancia con las posturas manifestadas a nivel europeo, esta Agencia, tal y como se refleja en nuestros informes 36/2020 y 31/2019. De este modo, el tratamiento de dichos datos, tanto en el ámbito del RGPD como de 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, y conforme a la doctrina del Tribunal Constitucional, requerirá una norma con rango de ley que justificara específicamente en qué medida y en qué supuestos, el tratamiento de datos biométricos respondería a un interés público esencial, definiendo dicha norma legal, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, 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 técnicas, organizativas y procedimentales adecuadas, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

De este modo, en el hipotético caso de que se apruebe la correspondiente norma legal que legitime el tratamiento de otros datos biométricos, podrá procederse a la modificación del contenido del Registro Central de Penados, lo que se puede hacer por la misma ley, teniendo en cuenta que los preceptos contenidos en el Título I no tienen naturaleza orgánica, por lo que no necesitarán en todo caso de una norma de dicho carácter. Pero sin prejuzgar ya, desde este momento, que la legislación nacional pueda habilitar dichos tratamientos que, en todo caso, quedarán sujetos a un análisis de riesgos y a la adopción de las garantías oportunas.

La siguiente cuestión que debe precisarse en relación con la protección de datos personales es la relativa a la normativa que resulta aplicable a los Registros, respecto de la cual la MAIN, en su página 26, hace la siguiente consideración:

“Excluir del ámbito de aplicación de la reciente normativa europea en materia de protección de datos de carácter personal toda la información penal contenida en los Registros penales se realiza a los efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención”.

A este respecto, hay que tener en cuenta que la normativa sobre protección de datos personales en el ámbito penal, recogida en la reciente 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, por la que se ha procedido a la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, establece un régimen especial que ha de ser objeto de interpretación restrictiva, tal y como se señaló reiteradamente en nuestro Informe 29/2020 sobre el Anteproyecto de Ley Orgánica, recordando que la Directiva

“viene a configurar un régimen especial, al que se someterían únicamente los tratamientos que la misma regula, frente al régimen general de protección de datos que se recoge en el Reglamento general de protección de datos. Por este motivo, las disposiciones del mismo serán de aplicación a todos los tratamientos llevados a cabo dentro del ámbito de aplicación del derecho de la Unión y que no estén regulados específicamente por la Directiva, tal y como se desprende del ámbito de aplicación establecido en el artículo 2 del Reglamento”.

De este modo, y de acuerdo con los artículos 1 y 2 de la Directiva, la misma se aplica al tratamiento de datos personales por parte de las autoridades competentes a los fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública, debiendo interpretarse este último inciso en relación con las que tengan naturaleza penal, quedando excluidas la de carácter administrativo. Por consiguiente, se configuran dos requisitos cumulativos, que se trate de tratamientos realizados por quien ostente la condición de autoridad competente y para los fines señalados, de modo que faltando alguno de ellos, no se trataría de una norma de transposición de la Directiva y estaría extendiendo a supuestos no contemplados en la misma una regulación más restrictiva del derecho fundamental a la protección de datos personales que la establecida en

el RGPD, que sería la norma general aplicable a los tratamientos en los que no concurren esos requisitos. Todo ello sin perjuicio de que, al amparo del artículo 23 del RGPD y siempre que se justifique la concurrencia de alguno de los supuestos previstos en el mismo, puedan establecerse limitaciones a los derechos de los afectados, que deberán responder al principio de proporcionalidad, pero sin que sea extensible, sin más, una regulación más restrictiva prevista para un supuesto diferente, como es la contenida en la Directiva.

En el presente caso, en relación con el tratamiento de los datos por los correspondientes Registros, la condición de responsable del tratamiento le corresponde al Ministerio de Justicia conforme a las previsiones del Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia, y tiene como objetivo fundamental “servir de apoyo a la actividad de los órganos judiciales y del Ministerio Fiscal, órganos judiciales y del Ministerio Fiscal, de las Fuerzas y Cuerpos de Seguridad del Estado y Cuerpos de Policía de las comunidades autónomas con competencias plenas en materia de seguridad pública, y de otros órganos administrativos, en el ámbito de las competencias delimitadas en el presente real decreto” (artículo 2.1 del Real Decreto 95/2009).

Por consiguiente, el tratamiento de los datos personales en los correspondientes Registros corresponde a un responsable del tratamiento que no tiene la consideración de autoridad competente a los efectos de la Directiva (UE) 2016/680. Del mismo modo, el tratamiento no se realiza exclusivamente a los fines de la citada Directiva, sino que se contemplan igualmente otros fines diferentes.

Por lo tanto, no concurren los presupuestos para aplicar la normativa especial derivada de la Directiva (UE) 2016/680, sino que nos encontraríamos ante un supuesto de tratamiento de datos personales sujetos a las reglas generales del RGPD, sin perjuicio de que una vez comunicados los datos por el Registro a las autoridades competentes y a los fines de la Directiva, los mismos se rijan por la normativa especial contenida en la Ley Orgánica 7/2021. Se trataría, por consiguiente, de un supuesto de colaboración con las autoridades competentes, respecto del cual, en nuestro informe 29/2020, se consideraba que el

“tratamiento llevado a cabo por el sujeto obligado a comunicar los datos a una autoridad competente está sometido a las disposiciones del Reglamento general de protección de datos y no a las de la Directiva, sin perjuicio de que una vez comunicados los datos a la autoridad competente sí será aplicable a ese tratamiento lo establecido en la Directiva, pero sin que esa aplicación implique que el sujeto obligado se encuentra sujeto a las previsiones de ésta última, toda vez que la comunicación se habrá llevado a cabo al amparo del artículo 6.1 c) del reglamento”.

Este criterio lo corrobora el propio RGPD, que se contempla expresamente la existencia de estos Registros en su artículo 10:

“El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas”.

En este mismo sentido, el artículo 10 de la LOPDGDD señala lo siguiente:

Artículo 10. Tratamiento de datos de naturaleza penal.

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.
2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.
3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Por consiguiente, el tratamiento de datos por los Registros queda sujeto al RGPD y a la LOPDGDD, sin perjuicio de las especialidades en su regulación que se puedan introducir, así como las posibles limitaciones a los derechos de los afectados al amparo del artículo 23 del RGPD.

Limitaciones que, al establecerse por la normativa nacional, requerirán de una norma con rango de ley que prevea, además, las garantías oportunas,

conforme a la doctrina constitucional recogida, entre otras, en sus relevantes sentencias 292/2000, de 30 de noviembre, y 76/2019 de 22 de mayo, tal y como se analiza a continuación.

III

Tal y como resulta del apartado anterior, los tratamientos de datos personales por el Sistema de Registros queda sujeto a la normativa general sobre protección de datos de carácter personal, y en la medida en que los mismos se fundamentarán en el cumplimiento de una misión de interés público o de obligaciones legales, su régimen deberá establecerse por una norma con rango de ley, tal y como resulta de las previsiones del RGPD y la LOPDGDD y de la jurisprudencia del TJUE y de nuestro Tribunal Constitucional.

A este respecto, el artículo 8 de la LOPDGDD recoge el principio constitucional de reserva de ley:

Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.

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

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley

Asimismo, deberá tenerse en cuenta la doctrina constitucional recogida, fundamentalmente en las citadas 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, de modo que dicha norma con rango de ley *“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).

Asimismo, deberá establecer 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.

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].

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.

En el presente caso, los distintos Registros que forman parte del Sistema de registros administrativos de apoyo a la Administración de Justicia

encuentran su habilitación legal, además de en el citado artículo 10.2. de la LOPDGDD, en las distintas normas especiales que los prevén, tal y como se analizó en el informe de esta Agencia 564/2008:

“Como igualmente se ha indicado, la legitimación para el tratamiento de los datos en los distintos registros ya ha sido objeto de análisis por esta Agencia Española de Protección de Datos en los diversos informes emitidos en relación con las normas sectoriales reguladoras de aquéllos

Así, en relación con el Registro Central de Penados y Rebeldes, el informe de 26 de julio de 2005 señalaba lo siguiente:

“(…) la inclusión de los datos en el Registro Central de Penados y Rebeldes será posible en cuanto exista una norma con rango de Ley que habilite el tratamiento en el Registro de los mencionados datos.

El 252 de la Ley de Enjuiciamiento Criminal dispone que “Los Tribunales remitirán directamente al Registro Central de Procesados y Penados, establecido en el Ministerio de Gracia y Justicia, notas autorizadas de las sentencias firmes en las que se imponga alguna pena por delito, y de los autos en que se declare la rebeldía de los procesados, con arreglo a los modelos que se les envíen al efecto”.

En consecuencia, el tratamiento de los datos en el Registro será posible en tanto se encuentra habilitado por dicho precepto o por otra norma con rango de Ley.”

Y en relación con los datos de sentencias firmes procedentes de órganos judiciales de otros Estados se señalaba que:

“En cuanto al tratamiento que se realice en virtud de los supuestos previstos en el artículo 6, el mismo será posible siempre que venga determinado por lo establecido en un Convenio Internacional, que forme parte del ordenamiento español en virtud de lo dispuesto en el artículo 95 de la Constitución.”

Esta conclusión debe reiterarse en este caso en relación con lo dispuesto en el artículo 3 del Proyecto ahora sometido a informe.

Igualmente, en relación con el Registro de Rebeldes Civiles, el informe de 17 de abril de 2001 señalaba lo siguiente:

“Por otra parte la inclusión de los datos en el fichero supondrá un tratamiento de datos de carácter personal, que, lógicamente dadas las circunstancias de rebeldía de los afectados, no contará con el consentimiento de aquéllos. No obstante, debe recordarse que el

artículo 6.1 de la Ley Orgánica 15/1999 admite el tratamiento inconsentido de los datos de carácter personal en aquéllos supuestos en que exista una norma con rango de Ley habilitante del tratamiento, siendo en este caso norma habilitante el artículo 157.1 de la Ley de Enjuiciamiento Civil, aplicable no sólo a la primera inscripción, sino a las ulteriores que se practiquen de conformidad con lo establecido en el artículo 3.3 del Proyecto.”

En cuanto al Registro de Sentencias de Responsabilidad Penal de los Menores, debe recordarse que la Disposición adicional tercera de la Ley Orgánica 5/2000, de 12 enero dispone que “en el Ministerio de Justicia se llevará un Registro de sentencias firmes dictadas en aplicación de lo dispuesto en la presente Ley, cuyos datos sólo podrán ser utilizados por los Jueces de Menores y por el Ministerio Fiscal a efectos de lo establecido en los artículos 6, 30 y 47 de esta Ley, teniendo en cuenta lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y sus disposiciones complementarias”, existiendo igualmente una habilitación legal para el tratamiento de los datos.

Por su parte, en relación con el Registro de Protección de las Víctimas de la Violencia Doméstica, la Disposición adicional primera de la Ley 27/2003, de 31 julio, establece que “el Gobierno, a propuesta del Ministerio de Justicia, oído el Consejo General del Poder Judicial y la Agencia de Protección de Datos, dictará las disposiciones reglamentarias oportunas relativas a la organización del Registro Central para la Protección de las Víctimas de la Violencia Doméstica, así como al régimen de inscripción y cancelación de sus asientos y el acceso a la información contenida en el mismo, asegurando en todo caso su confidencialidad”.

Igualmente, el apartado 8 del artículo *Artículo 544.ter. de la Ley de Enjuiciamiento Criminal* señala, en relación con la Orden de protección, que la misma “será notificada a las partes, y comunicada por el juez inmediatamente, mediante testimonio íntegro, a la víctima y a las Administraciones públicas competentes para la adopción de medidas de protección, sean éstas de seguridad o de asistencia social, jurídica, sanitaria, psicológica o de cualquier otra índole. A estos efectos se establecerá reglamentariamente un sistema integrado de coordinación administrativa que garantice la agilidad de estas comunicaciones”. Además, conforme al apartado 10 “la orden de protección será inscrita en el Registro Central para la Protección de las Víctimas de la Violencia Doméstica”.

Todo ello legitima el tratamiento de los datos en el citado Registro.

VII

Por último, debe hacerse especial referencia a la creación del Registro Central de Medidas cautelares, no prevista expresamente en una norma con rango de Ley, a fin de delimitar si el tratamiento de los datos que implica su existencia puede considerarse igualmente amparado por el artículo 6.1 de la Ley Orgánica 15/1999.

Tal y como recuerda la Exposición de Motivos del Proyecto, la existencia de este Registro encuentra su justificación en el necesario conocimiento por los órganos jurisdiccionales de la existencia de otras causas pendientes, requisitorias o medidas cautelares impuestas al acusado o procesado, a fin de lograr una aplicación adecuada de las normas penales y procesales, tanto en relación con la puesta en libertad o adopción de la medida de prisión provisional en fase de instrucción como para la determinación de la pena en fase de enjuiciamiento.

Así, en lo referente a la prisión provisional, dispone el apartado a) del artículo 503.1.3º de la Ley de Enjuiciamiento Criminal que

1. La prisión provisional sólo podrá ser decretada cuando concurren los siguientes requisitos:

3º Que mediante la prisión provisional se persiga alguno de los siguientes fines:

a) Asegurar la presencia del imputado en el proceso cuando pueda inferirse racionalmente un riesgo de fuga.

Para valorar la existencia de este peligro se atenderá conjuntamente a la naturaleza del hecho, a la gravedad de la pena que pudiera imponerse al imputado, a la situación familiar, laboral y económica de éste, así como a la inminencia de la celebración del juicio oral, en particular en aquellos supuestos en los que procede incoar el procedimiento para el enjuiciamiento rápido regulado en el título III del libro IV de esta Ley.

Procederá acordar por esta causa la prisión provisional de la persona imputada cuando, a la vista de los antecedentes que resulten de las actuaciones, hubieran sido dictadas al menos dos requisitorias para su llamamiento y busca por cualquier órgano judicial en los dos años anteriores. En estos supuestos no será aplicable el límite que respecto de la pena establece el ordinal 1º de este apartado.”

Asimismo, el artículo 66.1.6º del Código Penal establece, para la determinación de la pena a imponer que “cuando no concurren

atenuantes ni agravantes aplicarán la pena establecida por la Ley para el delito cometido, en la extensión que estimen adecuada, en atención a las circunstancias personales del delincuente y a la mayor o menor gravedad del hecho”.

Además, será posible la suspensión de la ejecución de la pena privativa de libertad, según el párrafo segundo del artículo 80.1 del propio Código, en atención “a la peligrosidad criminal del sujeto, así como a la existencia de otros procedimientos penales contra éste”.

Por último, según el artículo 81 del Código Penal serán condiciones necesarias para dejar en suspenso la ejecución de la pena, las siguientes:

“1ª Que el condenado haya delinquido por primera vez. A tal efecto no se tendrán en cuenta las anteriores condenas por delitos imprudentes ni los antecedentes penales que hayan sido cancelados, o debieran serlo, con arreglo a lo dispuesto en el artículo 136 de este Código.

2ª Que la pena o penas impuestas, o la suma de las impuestas, no sea superior a dos años, sin incluir en tal cómputo la derivada del impago de la multa.

3ª Que se hayan satisfecho las responsabilidades civiles que se hubieren originado, salvo que el Juez o Tribunal sentenciador, después de oír a los interesados y al Ministerio Fiscal, declare la imposibilidad total o parcial de que el condenado haga frente a las mismas.”

Lo dispuesto en el artículo 6.1 de la Ley Orgánica 15/1999 ha de complementarse con lo establecido en el artículo 10.2 del Reglamento de desarrollo de la misma, en cuya virtud “será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando (...) lo autorice una norma con rango de Ley o una norma de derecho comunitario y, en particular, cuando concorra uno de los supuestos siguientes:

- El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

- El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.”

Pues bien, aún cuando no existe una norma con rango de Ley que prevé expresamente la existencia de Registro de Medidas Cautelares, su contenido resulta necesario para que por los órganos jurisdiccionales del orden penal pueda darse pleno cumplimiento a las normas de la Ley de Enjuiciamiento Criminal y del Código Penal que acaban de ser reproducidas, dado que dichos órganos deberán conocer las circunstancias personales del acusado, imputado o reo y, en particular la existencia de causas penales o requisitorias dirigidas contra los mismos, para lo cual resulta necesario el establecimiento de un fichero en que se hagan constar estas circunstancias y que pueda ser objeto de consulta por aquéllos.

Por tanto, cabe considerar que, aún cuando sería aconsejable que existiese una norma con rango de Ley que previese expresamente su existencia, en términos similares a los que se prevé para los restantes registros integrantes del sistema, el tratamiento de datos derivado de la creación del Registro de Medidas cautelares se encontraría habilitado por el artículo 6.1 de la Ley Orgánica 15/1999 en conexión con las normas penales y procesales que acaban de reproducirse”.

No obstante lo anterior, teniendo en cuenta los requisitos exigidos por la actual normativa sobre protección de datos y la doctrina jurisprudencial aplicable, especialmente la recogida en la Sentencia del Tribunal Constitucional 76/2019, de 22 de mayo, posterior a la entrada en vigor de la LOPDGDD, esta Agencia entiende que sería deseable que el régimen jurídico aplicable al Sistema de Registros, con las especificidades propias de cada uno de ellos, se abordara en una norma con rango de ley que procediera a su regulación completa, limitándose en el anteproyecto de ley objeto de informe a realizar las modificaciones imprescindibles para la adecuada transposición de la Directiva (UE) 2019/884 y para la adaptación al Reglamento (UE) 2019/816.

IV

Sin perjuicio de lo anterior, se continúan analizando las principales cuestiones planteadas por el texto propuesto, refiriéndonos a las cautelas que prevé para el intercambio de datos para fines distintos del proceso penal, tanto en lo referente a las consultas que a través del Registro Central de Penados realicen Organismos Públicos españoles, como las que se reciban de otras autoridades centrales de la UE.

A estos efectos, se modifica el apartado 1 del artículo 10, incluyendo el siguiente párrafo:

“Cuando la finalidad de dicha consulta sea utilizar la información para fines distintos de un proceso penal, será necesario contar con el

consentimiento expreso de la persona sobre la que se realiza la consulta, salvo que una norma estatal con rango de ley lo exceptúe.”

Asimismo, se modifica el artículo 11:

5. Si la solicitud de información penal fuera para fines distintos de un procedimiento penal, el Registro Central de Penados transmitirá a la autoridad central del Estado requirente la información penal que no estuviese reservada a Jueces y Tribunales, siempre que se acredite el consentimiento expreso del interesado, salvo que el mismo no fuera necesario conforme al Derecho español para procedimientos de idéntica naturaleza.

En tal caso, el Registro Central de Penados transmitirá las condenas pronunciadas contra ciudadanos españoles que figuren inscritas siempre que el Estado de condena no se hubiera opuesto a esa retransmisibilidad, en cuyo caso se informará al Estado requirente acerca del Estado en que se dictó la condena, a los efectos oportunos.»

Esta Agencia valora positivamente las cautelas adoptadas, si bien, partiendo del principio actual de igualdad de todas las bases jurídicas contempladas en el artículo 6 del RGPD y el desplazamiento por el RGPD del tradicional “principio del consentimiento” que prevalecía en la normativa anterior, la existencia de otras bases, como pueda ser el interés público o el cumplimiento de obligaciones legales, no es propiamente una excepción al consentimiento, por lo que debería entenderse que la comunicación procederá, cuando no conste el consentimiento expreso, si estuviera amparada por una norma con rango de ley.

V

Por último, procede hacer referencia a la modificación de la disposición adicional tercera de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores, relativa al Registro Central de Menores, que incluirá además de las sentencias, las medidas cautelares, requisitorias y rebeldías, remitiendo el acceso a los datos al Real Decreto 95/2009, de 6 de febrero:

“Disposición adicional tercera. Creación del Registro Central de Menores.

En el Ministerio de Justicia se llevará un Registro Central de sentencias, medidas cautelares, requisitorias y rebeldías dictadas o acordadas en todos los procesos tramitados con arreglo a la presente Ley Orgánica. El

acceso a los datos de este Registro se ajustará a lo establecido en el Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia y en el Real Decreto 1110/2015 de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales, teniendo en cuenta la legislación aplicable en materia de protección de datos personales.

Hasta el momento de su creación, la inscripción de las sentencias firmes seguirá llevándose a cabo en el Registro de Sentencias de Responsabilidad Penal de los Menores. Las medidas cautelares, requisitorias y rebeldías se inscribirán en el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes, salvo las acordadas en los procedimientos seguidos en relación a alguna de las personas a las que se refiere el artículo 173.2 del Código Penal, cuya inscripción se llevará a cabo en el Registro Central para la Protección de las Víctimas de la Violencia Doméstica y de Género.”

La norma objeto de informe tiene el rango adecuado para la creación del citado Registro. No obstante, en relación con la remisión al Real Decreto 95/2009 y la conveniencia de regular en una norma con rango de ley los elementos básicos y fundamentales de los tratamientos de datos personales sobre datos relacionados con condenas penales, nos remitimos a lo indicado en el apartado III de este informe.