

N/REF: 0043/2023

La consulta plantea si es conforme a la normativa sobre protección de datos personales la comunicación de datos relativos a antecedentes policiales de los progenitores de menores de edad a los equipos técnicos de la Administración competente a efectos de valorar si puede existir un riesgo social para el menor o una situación de desamparo.

I

Para la adecuada resolución de la consulta debe partirse del diferente régimen jurídico al que pueden encontrarse sometido los ficheros policiales atendiendo a la concreta finalidad a la que estén destinados.

De este modo, aquellos ficheros que tengan por finalidad la prevención, detección o investigación de infracciones penales quedarán sujetos al régimen especial recogido en 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.

Tal y como señaló esta Agencia en el Informe 29/2022 sobre el anteproyecto de ley, la Directiva 2016/680 del Parlamento Europeo y del Consejo, cuya transposición se lleva a cabo por la misma “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”. Asimismo, se destacaba que el carácter de norma especial era igualmente predicable respecto de la norma que adapte el derecho español al Reglamento General de Protección de Datos (RGPD), constituida en el presente momento por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), cuyas disposiciones deberían ser tenidas en cuenta al constituir “la *lex generalis* aplicable para garantizar el derecho fundamental a la protección de datos de carácter personal”.

Por otro lado, dicho informe especificaba cómo su ámbito de aplicación quedaba limitado a las infracciones y sanciones penales, de modo que cualquier tratamiento en relación con la prevención de amenazas a la seguridad pública que puedan constituir infracciones administrativas se regulará conforme al RGPD, que establece mayores derechos para los interesados.

Partiendo de estas consideraciones el artículo 3.2.a) de la ley excluye de su ámbito de aplicación los siguientes tratamientos de datos personales:

a) Los realizados por las autoridades competentes para fines distintos de los previstos en el artículo 1, incluidos los fines de archivo por razones de interés público, investigación científica e histórica o estadísticos. Estos tratamientos se someterán plenamente a lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), así como en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

Por otro lado, como aplicación concreta del principio de limitación de la finalidad, el artículo 6.2. señala lo siguiente:

2. Los datos personales recogidos por las autoridades competentes no serán tratados para otros fines distintos de los establecidos en el artículo 1, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión Europea o por la legislación española. Cuando los datos personales sean tratados para otros fines, se aplicará el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión Europea

Por consiguiente, la comunicación de datos personales incluidos en los ficheros policiales a la que se refiere la consulta, en la medida en que supone un tratamiento de datos personales con un fin distinto de la prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública, requiere que esté autorizado por el Derecho de la Unión Europea o por la legislación española, quedando sometido al RGPD y a la LOPDGDD.

Esta previsión de norma legal específica que autorice el tratamiento se corresponde, asimismo, con la previsión contenida en el artículo 10 del RGPD respecto del tratamiento de datos personales relativos a condenas e infracciones penales:

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.

Dicho precepto se complementa con lo dispuesto en el artículo 10 de la LOPDGDD:

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.

Asimismo, deben tenerse en cuenta determinadas cautelas que establece la Ley Orgánica 7/2021 con la finalidad de que no se vean perjudicadas las investigaciones en curso. En este sentido, el artículo 7.4. de la ley, al regular el deber de colaboración con las autoridades competentes, prevé “que el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber facilitado el acceso a los mismos por

dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora” y que “Con el mismo propósito, los sujetos a los que el ordenamiento jurídico imponga un deber específico de colaboración con las autoridades competentes para el cumplimiento de los fines establecidos en el artículo 1, no informarán al interesado de la transmisión de sus datos a dichas autoridades, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, en cumplimiento de sus obligaciones específicas”. Asimismo, el artículo 24 regula las restricciones a los derechos de los afectados cuando resulte necesario y proporcional para la consecución de los siguientes fines:

- a) Impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales.*
- b) Evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales.*
- c) Proteger la seguridad pública.*
- d) Proteger la Seguridad Nacional.*
- e) Proteger los derechos y libertades de otras personas.*

Dicho régimen jurídico se completa con una serie de garantías determinantes de la licitud del tratamiento, incluidas obligaciones específicas a responsables y encargados y normas concretas para las transferencias internacionales de datos personales.

Atendiendo a dicha regulación especial, esta Agencia considera necesario para que proceda la comunicación de dichos datos a la que se refiere la consulta, además de que esté prevista por el Derecho de la Unión Europea o por la legislación española, tal y como se analizará posteriormente, que para la realización de la misma se valore si no se perjudican dichos fines y se realice con las cautelas necesarias para evitar que se frustren los fines a los que responde la Ley Orgánica 7/2021 o se desvirtualicen las concretas garantías que la misma establece.

II

En cuanto a los ficheros que contengan datos recogidos para fines administrativos, queda sujetos directamente al régimen general previsto en el RGPD y la LOPDGD. En este caso, la comunicación deberá ampararse en una base jurídica del artículo 6.1 del RGPD, que conforme al criterio de esta Agencia al referirse a tratamientos de datos personales por las

Administraciones Públicas, vendrá determinada bien por la letra c) o por la letra e) o por ambas:

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

En ambos supuestos, tal y como establece el artículo 6.2., la base jurídica deberá establecerse por el Derecho de la Unión o de los Estados miembros:

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

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

En el caso de tratarse de una norma nacional, la misma deberá tener rango de ley, tal y como recuerda el artículo 8 de la LOPDGDD:

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, deben tenerse en cuenta las prevenciones que, respecto de las posibles infracciones y sanciones administrativas, se establecen en el artículo 27 de la LOPDGDD:

Artículo 27. Tratamiento de datos relativos a infracciones y sanciones administrativas.

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas 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.

III

Por consiguiente, la comunicación de datos relativos a antecedentes policiales de los progenitores de menores de edad a los equipos técnicos de la Administración competente a efectos de valorar si puede existir un riesgo social para el menor o una situación de desamparo requiere que la misma se encuentre contemplada en una norma con rango de ley que contenga garantías específicas.

A este respecto, procede recordar la doctrina jurisprudencial del Tribunal Constitucional y del TJUE referida a la limitación del derecho fundamental a la protección de datos personales.

De acuerdo con la misma, el derecho a la protección de datos personales es un derecho fundamental, cuyo contenido consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso» (STC76/2019, de 22 de mayo, y STC 292/2000, de 30 de noviembre). Pero, además, estas sentencias señalaron igualmente la necesidad de que la injerencia esté prevista en una ley o norma de la Unión Europea, con respeto, en todo caso, al principio de proporcionalidad.

En concreto, el Tribunal Constitucional, en la STC 76/2019, de 22 de mayo, tras citar, entre otras, a su anterior STC 292/2000, de 30 de noviembre, señala:

- En segundo lugar, 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 (art. 81.1 CE), ora limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril, FJ 4). En la STC 49/1999, FJ 4, definimos la función constitucional de esa reserva de ley en los siguientes términos:

Esa reserva de ley a que, con carácter general, somete la Constitución española la regulación de los derechos fundamentales y libertades públicas reconocidos en su Título I, desempeña una doble función, a saber: de una parte, asegura que los derechos que la Constitución atribuye a los ciudadanos no se vean afectados por ninguna injerencia estatal no autorizada por sus representantes; y, de otra, en un Ordenamiento jurídico como el nuestro en el que los Jueces y Magistrados se hallan sometidos "únicamente al imperio de la Ley" y no existe, en puridad, la vinculación al precedente (SSTC 8/1981, 34/1995, 47/1995 y 96/1996) constituye, en definitiva, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los

derechos fundamentales y las libertades públicas. Por eso, en lo que a nuestro Ordenamiento se refiere, hemos caracterizado la seguridad jurídica como una suma de legalidad y certeza del Derecho (STC 27/1981, fundamento jurídico 10)."

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).

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; STC 66/1995, de 8 de mayo, F. 5; STC 55/1996, de 28 de marzo, FF. 7, 8 y 9; STC 270/1996, de 16 de diciembre, F. 4.e; STC 37/1998, de 17 de febrero, F. 8; STC 186/2000, de 10 de julio, 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].

Como ya mencionamos más arriba en este informe, la STC 76/2019, tan reiterada, dispone:

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).

Más recientemente, la Sentencia del TJUE (Gran Sala) de 21 de junio de 2022, al pronunciarse respecto de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, recuerdo su propia doctrina en los siguientes términos:

112 Hay que tener en cuenta que los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta no son derechos absolutos, sino que deben considerarse en relación con su función en la sociedad (Dictamen 1/15 (Acuerdo PNR UE-Canadá) de 26 de julio de 2017, EU:C:2017:592, apartado 136 -y jurisprudencia citada, y sentencia

de 6 de octubre de 2020, *Privacy International*, C623/17-, EU:C:2020:790, apartado 63 y jurisprudencia citada).

113 Según la primera frase del apartado 1 del artículo 52 de la Carta, toda limitación del ejercicio de los derechos y libertades reconocidos por la Carta debe estar prevista por la ley y respetar la esencia de dichos derechos y libertades. En virtud de la segunda frase del apartado 1 del artículo 52 de la Carta, y sin perjuicio del principio de proporcionalidad, sólo pueden establecerse limitaciones a estos derechos y libertades si son necesarias y responden realmente a objetivos de interés general reconocidos por la Unión Europea o a la necesidad de proteger los derechos y libertades de los demás. A este respecto, el apartado 2 del artículo 8 de la Carta establece que los datos personales deben tratarse, entre otras cosas, "con fines determinados y sobre la base del consentimiento del interesado o en virtud de otro fundamento legítimo previsto por la ley".

*114 Debe añadirse que la exigencia de que toda limitación del ejercicio de los derechos fundamentales esté prevista por la ley implica que el acto que permite la injerencia en dichos derechos debe definir por sí mismo el alcance de la limitación del ejercicio del derecho de que se trate, teniendo en cuenta, por una parte, que esta exigencia no se opone a que la limitación de que se trate se formule en términos suficientemente abiertos para poder adaptarse a los distintos supuestos y seguir el ritmo de la evolución de las circunstancias (véase, en este sentido, la sentencia de 26 de abril de 2022, *Polonia/Parlamento y Consejo*, C401/19-, EU:C:2022:297, apartados 64 y 74 y la jurisprudencia citada) y, por otra parte, que el Tribunal de Justicia puede, en su caso, precisar, por vía interpretativa, el alcance efectivo de la limitación a la luz del propio tenor de la normativa de la UE en cuestión, así como de su régimen general y de los objetivos que persigue, interpretados a la luz de los derechos fundamentales garantizados por la Carta.*

115 Por lo que respecta a la observancia del principio de proporcionalidad, la protección del derecho fundamental al respeto de la vida privada en el ámbito de la UE exige, según reiterada jurisprudencia del Tribunal de Justicia, que las excepciones y limitaciones a la protección de datos personales sólo se apliquen en la medida estrictamente necesaria. Además, un objetivo de interés general no puede perseguirse sin tener en cuenta que debe conciliarse con los derechos fundamentales afectados por la medida, ponderando adecuadamente el objetivo de interés general con los derechos en cuestión [Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 140, y sentencia de 5 de abril de 2022,

Commissioner of An Garda Síochána y otros, C140/20-, EU:C:2022:258, apartado 52 y jurisprudencia citada].

116 Más concretamente, la cuestión de si los Estados miembros pueden justificar una limitación de los derechos garantizados en los artículos 7 y 8 de la Carta debe apreciarse midiendo la gravedad de la injerencia que tal limitación supone y verificando que la importancia del objetivo de interés general perseguido por dicha limitación es proporcional a dicha gravedad (véanse, en este sentido, las sentencias de 2 de octubre de 2018, Ministerio Fiscal, C207/16-, EU:C:2018:788, apartado 55 y la jurisprudencia citada, y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C140/20, EU:C:2022:258, apartado 53 y la jurisprudencia citada).

117 Para cumplir el requisito de proporcionalidad, la legislación en cuestión que implique la injerencia debe establecer normas claras y precisas que regulen el alcance y la aplicación de las medidas previstas e impongan unas garantías mínimas, de modo que las personas cuyos datos hayan sido transferidos dispongan de garantías suficientes para proteger eficazmente sus datos personales contra el riesgo de abuso. En particular, debe indicar en qué circunstancias y bajo qué condiciones puede adoptarse una medida que prevea el tratamiento de dichos datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de estas garantías es aún mayor cuando los datos personales son objeto de tratamiento automatizado. Estas consideraciones se aplican especialmente cuando los datos del PNR pueden revelar datos sensibles de los pasajeros (Dictamen 1/15 (Acuerdo PNR UE-Canadá) de 26 de julio de 2017, -EU:C:2017:592, apartado 141, y sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C511/18-, C512/18 -y C520/18-, EU:C:2020:791, apartado 132 y la jurisprudencia citada).

118 Así, la legislación que prevé la conservación de datos personales debe seguir satisfaciendo criterios objetivos que establezcan una conexión entre los datos que deben conservarse y el objetivo perseguido (véanse, en este sentido, el Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 191 y la jurisprudencia citada, y las sentencias de 3 de octubre de 2019, A y otros, C70/18, EU:C:2019:823, apartado 63, y de 6 de octubre de 2020, La Quadrature du Net y otros, C511/18-, C512/18 -y C520/18-, EU:C:2020:791, apartado 133).

IV

La Ley Orgánica 1/1996 de 15 de enero de Protección Jurídica del Menor regula en el Capítulo I del Título II las actuaciones en situaciones de desprotección social del menor, entre ellas las actuaciones de protección y ante situaciones de riesgo y de desamparo.

Tras la reforma operada por la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, se incorporó un artículo 22 quáter que introduce normas que regulan el tratamiento de datos de carácter personal atendiendo al interés superior del menor:

Artículo 22 quáter. Tratamiento de datos de carácter personal.

1. Para el cumplimiento de las finalidades previstas en el capítulo I del título II de esta ley, las Administraciones Públicas competentes podrán proceder, sin el consentimiento del interesado, a la recogida y tratamiento de los datos que resulten necesarios para valorar la situación del menor, incluyendo tanto los relativos al mismo como los relacionados con su entorno familiar o social.

Los profesionales, las Entidades Públicas y privadas y, en general, cualquier persona facilitarán a las Administraciones Públicas los informes y antecedentes sobre los menores, sus progenitores, tutores, guardadores o acogedores, que les sean requeridos por ser necesarios para este fin, sin precisar del consentimiento del afectado.

2. Las entidades a las que se refiere el artículo 13 podrán tratar sin consentimiento del interesado la información que resulte imprescindible para el cumplimiento de las obligaciones establecidas en dicho precepto con la única finalidad de poner dichos datos en conocimiento de las Administraciones Públicas competentes o del Ministerio Fiscal.

3. Los datos recabados por las Administraciones Públicas podrán utilizarse única y exclusivamente para la adopción de las medidas de protección establecidas en la presente ley, atendiendo en todo caso a la garantía del interés superior del menor y sólo podrán ser comunicados a las Administraciones Públicas que hubieran de adoptar las resoluciones correspondientes, al Ministerio Fiscal y a los órganos judiciales.

4. Los datos podrán ser igualmente cedidos sin consentimiento del interesado al Ministerio Fiscal, que los tratará para el ejercicio de las funciones establecidas en esta ley y en la normativa que le es aplicable.

5. En todo caso, el tratamiento de los mencionados datos quedará sometido a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus disposición de desarrollo, siendo exigible la implantación de las medidas de seguridad de nivel alto previstas en dicha normativa.

La redacción de dicho precepto responde a las observaciones que se realizaron por esta Agencia al anteproyecto de ley en el Informe 195/2014 y

recoge literalmente la propuesta de redacción realizada, que se justificaba del siguiente modo:

XI

Debe por último hacerse referencia a los tratamientos de datos derivados de las distintas actuaciones administrativas de protección del menor en situaciones de riesgo y desamparo que establece el Anteproyecto.

Así, por ejemplo, el artículo 17.4, en la redacción propuesta por el Anteproyecto, dispone que “la valoración de la situación de riesgo conllevará la elaboración y puesta en marcha de un proyecto de intervención socio-familiar que deberá recoger las actuaciones, recursos y previsión de plazos, promoviendo los factores de protección del menor y manteniendo a éste en su entorno familiar. Se comunicará a los padres, tutores, guardadores o acogedores la valoración de la situación de riesgo y el proyecto de intervención y serán oídos y tenida en cuenta su opinión, así como la del menor si tiene suficiente madurez y, en todo caso, a partir de los 12 años, para que, si es posible, pueda consensuarse dicho proyecto, recogándose en un convenio suscrito entre el órgano competente y los padres, tutores, guardadores o acogedores”.

Además, el apartado 7 establece que “Cuando la Administración Pública competente esté desarrollando una intervención ante una situación de riesgo de un menor y tenga noticia de que va a ser trasladado al ámbito de otra Entidad territorial, la Administración Pública de origen lo pondrá en conocimiento de la de destino al efecto de que, si procede, ésta continúe la intervención que se venía realizando, con remisión de la información y documentación necesaria. Si la Administración Pública de origen desconociera el lugar de destino, podrá solicitar el auxilio de las Fuerzas y Cuerpos de Seguridad a fin de que procedan a su averiguación. Una vez conocida la localización del menor, se pondrá en conocimiento de Entidad Pública competente en dicho territorio, que continuará la intervención”. También se prevén normas de comunicación de la información entre las Administraciones competentes en la redacción propuesta del artículo 18.4.

En el ámbito del acogimiento familiar, el artículo 20.3 e) de la Ley Orgánica, también en la redacción propuesta, prevé que a la resolución

dictada por la Entidad Pública que tenga la tutela o guarda se acompañará “El contenido del seguimiento que, en función de la finalidad del acogimiento, vaya a realizar la Entidad Pública y el compromiso de colaboración con dicho seguimiento por parte de la familia acogedora”.

Todo ello, unido a las competencias de las Administraciones Públicas a las que se refiere la Ley implica necesariamente que por parte de las mismas se recogerán, tratándose de situaciones de riesgo de las descritas en el Capítulo I del Título II datos de carácter personal no sólo referidos a aquél, sino a también a quienes integran su núcleo familiar o incluso referidos a su entorno social. Además, debe tenerse en cuenta que de los tres primeros apartados del artículo 13, inalterados por el Anteproyecto sometido a informe, se deriva la comunicación a dichas autoridades de informaciones referidas al menor y el citado entorno familiar, escolar o social, por cuanto establecen lo siguiente:

“1. Toda persona o autoridad, y especialmente aquellos que por su profesión o función, detecten una situación de riesgo o posible desamparo de un menor, lo comunicarán a la autoridad o sus agentes más próximos, sin perjuicio de prestarle el auxilio inmediato que precise.

2. Cualquier persona o autoridad que tenga conocimiento de que un menor no está escolarizado o no asiste al centro escolar de forma habitual y sin justificación, durante el período obligatorio, deberá ponerlo en conocimiento de las autoridades públicas competentes, que adoptarán las medidas necesarias para su escolarización.

3. Las autoridades y las personas que por su profesión o función conozcan el caso actuarán con la debida reserva.

En las actuaciones se evitará toda interferencia innecesaria en la vida del menor.”

Como ya se ha indicado en el apartado III de este informe, han sido numerosos los supuestos en los que se ha planteado a esta Agencia la licitud de la recogida de las informaciones necesarias para atender a situaciones especiales de riesgo, desamparo o exclusión social de menores de edad no sólo por las Administraciones

competentes, sino también por quienes se encuentran sometidos al deber de colaboración al que se acaba de hacer referencia.

A tal efecto, ya se ha indicado que debe tenerse particularmente en cuenta la protección del interés superior del menor, conciliándose además este principio, cuando se trata de la recogida de los datos del propio menor, con su derecho fundamental a la protección de datos de carácter personal.

Tratándose de la necesaria atención de los supuestos de riesgo y desamparo a los que está haciéndose ahora referencia podría considerarse que el tratamiento de los datos del menor y de las personas que configuran su entorno puede resultar necesario para la adecuada valoración de sus circunstancias y la adopción de las medidas que resulten necesarias, en su caso, para atender a su interés superior. De este modo, sería posible considerar lícito el mencionado tratamiento. Ahora bien, el tratamiento debería quedar sujeto a una serie de garantías estrictas que asegurasen que la injerencia en el derecho del afectado, particularmente cuando es el propio menor es mínimo.

La primera de ellas sería la referida a la limitación absoluta de la finalidad del tratamiento que, en el caso de las Administraciones competentes debería quedar supeditada al cumplimiento de los fines derivados del régimen especial establecido en el propio Capítulo I del Título II de la Ley Orgánica 1/1996, mientras que en el de quienes se encuentren obligados a colaborar con aquéllas deberá supeditarse única y exclusivamente, al cumplimiento del mencionado deber de colaboración.

La segunda implicaría la limitación de las cesiones de datos que podrían resultar admisibles, que debería limitarse únicamente a las destinadas a las Administraciones Públicas competentes, el Ministerio Fiscal y los órganos del Poder Judicial.

Y la tercera, derivada de las anteriores, implicaría la necesaria adopción de medidas reforzadas de seguridad sobre los tratamientos que se llevaran a cabo. A tal efecto, debe tenerse especialmente en cuenta que esos tratamientos implicarán en general la recogida de una información ingente relacionada con la situación del menor y de su entorno, no siendo en modo alguno extraño que se incluyesen datos relacionados con su salud y origen racial, así como con la vida sexual de

quienes conforman su entorno familiar. De este modo, sería necesaria la implantación de las medidas de seguridad de nivel alto establecidas en la normativa de protección de datos.

Asimismo, el régimen de garantías específicas recogidas en el citado precepto se complementa, además, por el deber genérico de reserva recogido en el artículo 13.3 de la Ley Orgánica 1/1996.

Sin perjuicio de la transcrita previsión legal, debe tenerse en cuenta la doctrina del Tribunal Constitucional contraria al tratamiento masivo de datos personales por las Administraciones Públicas, recogida con claridad en su Sentencia 17/2013 de 31 de enero de 2013, en sus Fundamentos Jurídicos 7 y 8.

Señala el FJ7, referido al acceso por parte de los órganos competentes en materia de extranjería a los datos obrantes en poder de otros órganos administrativos:

En cuanto al segundo párrafo de la disposición adicional impugnada, el mismo autoriza a los órganos de la Administración estatal, competentes en el ámbito de los procedimientos administrativos que se tramiten en el ámbito que regula la Ley Orgánica de derechos y libertades de los extranjeros y solamente en el ejercicio de las competencias que tienen atribuidas, para acceder a los ficheros en los que obren datos necesarios para su actuación de la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social y el Instituto Nacional de Estadística, este último en lo relativo al padrón municipal de habitantes, lo cual ha de realizarse de acuerdo con la legislación sobre protección de datos sin que sea preciso el consentimiento del interesado. Al respecto, conviene hacer notar que la mención del precepto a los procedimientos administrativos tramitados en el ámbito de la Ley Orgánica de derechos y libertades de los extranjeros no puede entenderse sino haciendo referencia a la tramitación de un determinado expediente en el que resulta necesaria la constancia de determinado dato que ya obra en poder de otro órgano de la Administración General del Estado, tratándose así de un acceso específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo o indiscriminado. La finalidad de esa cesión no es otra que comunicar el contenido de ficheros con datos tributarios, de Seguridad Social o de residencia, datos que, en cualquier caso, son ya previamente conocidos por la Administración General del Estado, atendiendo a la necesidad de

que la misma disponga de la información oportuna para la gestión de procedimientos en materia de extranjería que son también de su competencia. Por ello, en la medida en que han de tratarse de datos relacionados con un concreto procedimiento y que ya obran en poder de la Administración pública, no puede considerarse vulnerado el art. 18.4 CE. En todo caso, como ya hemos señalado, tal acceso solamente puede producirse cuando ese dato resulte necesario o pertinente en relación con la tramitación de un concreto expediente, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen legal que le resulta de aplicación. Así, rectamente interpretada en los términos antes expuestos, resulta que esa cesión de datos que el acceso previsto supone ha de realizarse de acuerdo con lo que al respecto disponga la Ley Orgánica de protección de datos lo que determina, no solamente la aplicación de lo que la misma dispone en materia de información al interesado respecto de la cesión de datos (art. 5.4 LOPD), sino también que la cesión, establecida en una norma legal [art.11.2 a) LOPD], se produce para el cumplimiento de finalidades legítimas del órgano cedente y del cesionario (art. 4.1 LOPD), finalidades que, desde el punto de vista material, no resultan ser incompatibles entre sí (art. 4.2 LOPD), sino que, por el contrario, los datos son comunicados para el cumplimiento de fines directamente relacionados con las funciones legítimas de cedente y cesionario que contribuyen a garantizar un bien de relevancia constitucional: dar cumplimiento a lo dispuesto en la ley, en este caso la de extranjería (arts. 10.1 y 13.1 CE).

Asimismo, en su FJ 8, interpreta el artículo 16.3 de la Ley de Bases de Régimen Local para determinar la constitucionalidad del mismo. Tal y como ha sido interpretado por el TC en dicha sentencia (FJ 8), este precepto se refiere a la cesión no consentida de los datos relativos a la residencia o el domicilio a otras Administraciones públicas que así lo soliciten solamente en aquellos casos en los que, para el ejercicio de sus competencias, sean aquellos datos relevantes. En suma, esta petición, que no se refiere específicamente a la cesión de datos del padrón en lo concerniente a los datos de los extranjeros, tiene por finalidad poder disponer de los datos relativos a la residencia o el domicilio que constan en el padrón municipal, (...).De esta forma, de acuerdo con la Ley Orgánica de protección de datos, la finalidad inicial que justificó la recogida de los datos por parte de una Administración pública no impide el destino posterior de los datos para su uso en finalidades diferentes de aquellas que motivaron su recogida respetando, en todo caso, el principio de reserva de ley para establecer dicho cambio, (...) la Ley de bases de régimen local en su condición, además, de norma reguladora de un fichero como el padrón municipal puede prever cesiones de datos entre Administraciones públicas.

(...) los datos cedidos han de ser los estrictamente necesarios para el cumplimiento de las funciones asignadas a los órganos administrativos de forma que deberá motivarse la petición de aquellos datos que resulten relevantes, pues es necesario distinguir entre el análisis y seguimiento de una situación individualizada relativa a un caso concreto y el suministro generalizado e indiscriminado de toda la información contenida en un registro personal. El precepto ha contemplado ambos extremos de manera que cualquier cesión de los datos del padrón debe fundamentarse en la necesidad por parte de la Administración cesionaria actuando en el ejercicio de sus competencias, de conocer, en cada caso concreto, el dato relativo al domicilio de la persona afectada, extremos que han de ser adecuadamente valorados por la cedente a fin de apreciar si los datos que se solicita son realmente necesarios, pertinentes y proporcionados, atendiendo a la competencia que pretende ejercer la Administración cesionaria (art. 4 in fine de la Ley 30/1992). Se trata así de una regla de por sí restringida a los datos relativos a la residencia y al domicilio en cada caso concreto, y a la que le resultarán de aplicación, de más está decirlo, el resto de principios y previsiones que conforman el contenido del derecho reconocidos en la legislación sobre protección de datos.

De lo anteriormente transcrito, y del resto de la fundamentación jurídica contenida en dicha sentencia resulta que el TC ha determinado que (i) habrá de evitarse el acceso indiscriminado y masivo a los datos personales (ii) el dato en cuestión solicitado habrá de ser pertinente y necesario (iii) para la finalidad establecida en el precepto (iv) la solicitud de acceso a los concretos datos personales habrá de motivarse y justificarse expresamente, (v) de manera que ello posibilite su control por el cedente (vi) y se evite un uso torticero de esa facultad con accesos masivos. Ello supone (vii) que ha de quedar garantizada la posibilidad de analizar si en cada caso concreto el acceso tenía amparo en lo establecido en la ley.

Por consiguiente, no cabe un acceso masivo e indiscriminado a datos personales, y por lo tanto, en cambio, cuando exista la posibilidad de cesión establecida en una ley, como ocurre en el presente caso, dicho acceso deberá ser siempre “específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo e indiscriminado”; “tal acceso sólo podría producirse cuando ese dato resulte necesario o pertinente en relación con la tramitación de un concreto expediente, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen General que le resulte de aplicación.” (STC 19/2013, FJ 7º).

Consecuentemente la previsión legal del art. 22 quater de la Ley Orgánica 1/1996 no supone una habilitación genérica para la comunicación a la autoridad administrativa autonómica de todos los datos personales que puedan figurar en los ficheros policiales respecto del progenitor de un menor incurso en un procedimiento de posible declaración de la situación de desamparo, sino únicamente de aquellos datos que sean estrictamente necesarios en el seno del procedimiento tramitado por la autoridad autonómica para la adecuada protección de los menores por los poderes públicos mediante la prevención, detección y reparación de situaciones de riesgo, con el ejercicio de la guarda y, en los casos de declaración de desamparo, para la asunción de la tutela por ministerio de la ley.

De este modo, el requerimiento de tales datos por la Administración competente solamente podrá efectuarse cuando exista una situación comprobada de riesgo de exclusión social o desamparo del menor, lo que deberá ser suficiente y expresamente motivado y razonado por la Administración requirente.

En segundo lugar, la comunicación de datos que se efectúe estará sujeta al principio de minimización de datos, recogido en el artículo 5.1.c) del RGPD, según el cual los datos personales serán *adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados*, sin que se ampare las cesiones masivas de datos, quedando limitada a los datos necesarios para la determinación de la medida o medidas que en favor del menor en situación de exclusión o de riesgo vayan a aplicarse.

En tercer lugar el tratamiento de los datos así obtenidos estará sujeto estrictamente al principio de finalidad consagrado en el artículo 5.1.b) del RGPD, conforme al cual los datos personales serán *recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines*[...].

Por último, conforme al régimen de responsabilidad proactiva instaurado por el RGPD, la Administración autonómica deberá garantizar la aplicación de las medidas técnicas y organizativas que resulten de la correspondiente evaluación de impacto en la protección de datos, en los términos previstos en el artículo 3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

V

Para concluir deberá tenerse en cuenta, en su caso, las previsiones que pueda establecer la normativa legal autonómica, como ocurre en el presente caso con la normativa catalana, en el que la Ley 17/2010, de 27 de mayo, de

los derechos y las oportunidades en la infancia y la adolescencia recoge expresamente en el artículo 24.2 la comunicación de los datos policiales:

2. Las administraciones implicadas deben colaborar y actuar coordinadamente. Especialmente en materia de protección de los niños y los adolescentes, los servicios públicos están obligados a facilitar la información requerida por el departamento competente en materia de protección de los niños y los adolescentes a fin de valorar cuál es la situación del niño o el adolescente, y a llevar a cabo las actuaciones de colaboración necesarias para su protección. Los datos que pueden ser cedidos entre administraciones sin consentimiento de la persona afectada son las económicas, laborales, sociales, educativas, de salud, policiales y penales de los menores y de sus progenitores, tutores o guardadores.