

061/2024**I**

El proyecto sometido a informe tiene por objeto la introducción de varias modificaciones en el texto actual del Real Decreto 95/2009 (a su vez modificado por otras disposiciones anteriores) y consta de un artículo único y dos disposiciones finales en el que se recogen las modificaciones de los artículos 1, 2, 4, 5, 6, 7, 8, 9, 10, 16, 17, 18, 19, 21, 22, 26 y la creación del artículo 28, la Disposición adicional quinta, la Disposición adicional sexta y Disposición adicional séptima del citado Real Decreto por el que se regula el SIRAJ (Sistema de registros de apoyo a la Administración de Justicia)

No obstante lo anterior, y en coherencia con la materia que nos ocupa se hace necesario englobar de manera sistemática dichas modificaciones en dos grupos.

Un primer grupo relativo a distintas actualizaciones y adecuaciones a denominaciones actuales, ya sean de órganos o departamentos competentes (Disposición transitoria primera, la Disposición final segunda y la Disposición final tercera para actualización de la denominación del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes), de cuerpos de funcionarios (artículos 16 a); Disposición Adicional primera), de tipos de registros en los que se integra el SIRAJ (artículo 1.2), de nuevas denominaciones de tipificación de conductas e introducción de otros instrumentos jurídicos (artículo 2.3 a), b) y c); artículo 5.2; artículo 6.1 b; artículo 10 a), b) y d); artículo 17.7), así como la adaptación de la norma a un lenguaje inclusivo (artículos 6.2, 7.2 y 3; 16 b)) o incluso la modificación de plazos (artículo 19.2).

Y un segundo grupo de modificaciones que, directa o indirectamente, afecta al marco jurídico aplicable al tratamiento de datos de carácter personal, y que serán sobre los que se centre el presente informe.

II

Dicho lo anterior, con carácter previo es preciso delimitar el marco jurídico que resultaría de aplicación a los tratamientos de datos personales derivados de la aplicación de la norma proyectada y en concreto del funcionamiento del SIRAJ.

Debe partirse de que el SIRAJ, dada la variedad de registros que integra, contendrá datos “ordinarios” y datos de naturaleza penal, tal como se deduce del objeto del Real Decreto 95/2009.

Por tanto, se hace necesario determinar, en primer lugar, el contenido material del mismo, es decir, qué tipo de información se somete a tratamiento, y, en segundo término, para qué se tratan los datos, o dicho de otro modo a qué finalidad sirven y en consecuencia quién o quiénes son los actores intervinientes en dichos tratamientos.

En efecto, el Real Decreto 95/2009, en cuanto a su objeto, indica en el artículo 1.2 que el SIRAJ *estará integrado por el Registro Central de Penados, el Registro Central para la Protección de las Víctimas de la Violencia Doméstica y de Género, el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes, el Registro Central de Rebeldes Civiles, el Registro de Sentencias de Responsabilidad Penal de los Menores y el Registro Central de Delincuentes Sexuales.*

Y en su artículo 2.3 determina que, el SIRAJ, *está integrado por las bases de datos de los Registros que a continuación se relacionan, tiene por objeto, en cada caso:*

a) Registro Central de Penados: la inscripción de las resoluciones firmes por la comisión de un delito o falta que impongan penas o medidas de seguridad, dictadas por los Juzgados o Tribunales del orden jurisdiccional penal.

b) Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes: La inscripción de penas y medidas de seguridad impuestas en sentencia no firme por delito o falta y medidas cautelares acordadas que no sean objeto de inscripción en el Registro Central para la Protección de las Víctimas de la Violencia Doméstica y de Género, autos

de declaración de rebeldía y requisitorias adoptadas en el curso de un procedimiento penal por los Juzgados o Tribunales del orden jurisdiccional penal, anotándose la fecha de notificación cuando la misma se produzca.

c) Registro Central para la Protección de las Víctimas de la Violencia Doméstica y de Género: la inscripción de penas y medidas de seguridad impuestas en sentencia por delito o falta, medidas cautelares y órdenes de protección acordadas en procedimientos penales en tramitación, contra alguna de las personas a las que se refiere el artículo 173.2 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Asimismo, la inscripción de los quebrantamientos de cualquier pena, medida u orden de protección acordada en dichos procedimientos penales.

d) Registro Central de Rebeldes Civiles: la inscripción de demandados en cualquier procedimiento civil cuyo domicilio se desconozca y siempre que no hayan tenido resultado positivo las averiguaciones de domicilio a que se refiere el artículo 156 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

e) Registro Central de Sentencias de Responsabilidad Penal de los Menores: la inscripción de sentencias condenatorias firmes dictadas por los Juzgados y Tribunales en aplicación de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la Responsabilidad Penal de los Menores.

f) Registro Central de Delincuentes Sexuales: la inscripción de la información relativa a quienes hayan sido condenados por sentencia judicial firme por los delitos contra la libertad e indemnidad sexuales, así como por trata de seres humanos con fines de explotación sexual, incluyendo la pornografía, de conformidad con la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia.

Respecto de la segunda cuestión, el propio artículo 1 de la norma, establece que el objetivo fundamental del SIRAJ es servir de apoyo a la actividad de los 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.

Ahondando en este aspecto, en la página web del Portal del Servicio Público de Justicia¹ dependiente del Ministerio de Presidencia, Justicia y Relaciones con las Cortes se ofrece información sobre el SIRAJ de la que se deduce la pluralidad de destinatarios y funciones que cumple el sistema: desde Órganos Judiciales, Instituciones Penitenciarias, Fuerzas y Cuerpos de Seguridad del Estado, Dirección General de Tráfico (por ejemplo para el envío telemático a la DGT de la retirada del permiso de conducir e incautación de vehículos, intervención de los agentes en controles de carretera, etc.,...) la Seguridad Social y Clases Pasivas (por ejemplo para pensiones de viudedad ya que se envía semanalmente información para evitar que condenados por determinados delitos de violencia doméstica/género cobren pensiones tras la muerte de sus parejas o exparejas), para Universidades y Sanidad (intercambio europeo de condenados e inhabilitación profesional sanitaria/Educativa para evitar reincidencia internacional) e incluso para el propio ciudadano en multitud de trámites personales.

Por tanto, serán objeto de tratamiento en el SIRAJ tanto datos meramente identificativos como datos de naturaleza penal, y la finalidad del tratamiento -que resulta esencial para establecer el régimen jurídico aplicable- dependerá de la competencia del órgano o autoridad que va a acceder al mismo, todo ello sin perjuicio de las autoridades bajo las que se gestionen los distintos Registros en los que se integra el citado SIRAJ, dependiente en todo caso del actual Ministerio de Presidencia, Justicia y Relaciones con las Cortes.

III

Teniendo en cuenta lo anterior, el marco jurídico de protección de datos al que debe acudir es el RGPD, la LOPDGDD y 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.

Dispone el artículo 2.2 d) del RGPD lo siguiente:

¹ <https://www.administraciondejusticia.gob.es/-/soluciones-siraj-2>

2. *El presente Reglamento no se aplica al tratamiento de datos personales:*

(...)

d) por parte de las autoridades competentes con fines 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.

Dispone el artículo 10 del RGPD bajo la denominación "Tratamiento de datos personales relativos a condenas e infracciones penales" lo siguiente:

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.

La LOPDGDD en su artículo 10 bajo la denominación "Tratamiento de datos de naturaleza penal" dispone que:

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.

Por su parte, la Ley Orgánica 7/2021, de 26 de mayo, dispone en su artículo 1 que el objeto de la misma es

establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de 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.

Y continua en su artículo 2.2 que

El tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de las actuaciones o procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, en el ámbito del artículo 1, se regirá por lo dispuesto en la presente Ley Orgánica (...)

En cuanto a qué se entiende por “Autoridades competentes”, la ley dispone en su artículo 4 lo siguiente:

1. Será autoridad competente, a los efectos de esta Ley Orgánica, toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con alguno de los fines previstos en el artículo 1.

En particular, tendrán esa consideración, en el ámbito de sus respectivas competencias, las siguientes autoridades:

- a) Las Fuerzas y Cuerpos de Seguridad.*
- b) Las Administraciones Penitenciarias.*
- c) La Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria.*
- d) El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.*
- e) La Comisión de Vigilancia de Actividades de Financiación del Terrorismo.*

2. También tendrán consideración de autoridades competentes las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

Asimismo debe recordarse el concepto de tratamiento, que el RGPD en su artículo 4.2 considera *cualquier operación o conjunto de operaciones*

realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

Es decir, deben tenerse en cuenta, aunque sea a título ejemplificativo (“como”) los conceptos que cita el precepto pues en el SIRAJ podrán llevarse a cabo acciones de todo tipo y desde varios puntos de vista, no solo el acceso por parte de terceros, sino la propia aportación de datos que se realice desde las fuentes que nutren de información los distintos Registros que integran el SIRAJ, es decir, de órganos jurisdiccionales y de cuerpos y fuerzas de seguridad del estado.

La conclusión a la que se llega tras el análisis de los preceptos citados, y la naturaleza de los registros que integran el SIRAJ, es que, con carácter general la norma de protección de datos aplicable a dicho sistema será el RGPD, y la habilitación legal para el tratamiento la encontramos en el propio artículo 10 apartado 2 de la LOPDGDD que remite a *la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia*.

Así por ejemplo en nuestro Informe 26/2023 se estimó la aplicación del RGPD al Registro de Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos, que se integra en el SIRAJ, por entenderse que servía a la finalidad de *“contribuir a la protección de los menores contra la explotación y las agresiones sexuales, permitiendo conocer si quienes pretenden el acceso y ejercicio de profesiones, oficios y actividades que impliquen el contacto habitual con menores, carecen o no de condenas penales por cualquier delito contra la libertad sexual o por trata de seres humanos”*.

Ahora bien, dependiendo de la finalidad del tratamiento, el régimen jurídico aplicable podría ser la LO 7/2021.

En efecto, existirán supuestos en los que la norma de protección de datos aplicable a determinados tratamientos dependerá de quiénes accedan o sean destinatarios de la información en él contenida -ya que podemos encontrar tanto órganos judiciales, fuerzas y cuerpos de seguridad del Estado, pero también autoridades administrativas, y el propio ciudadano- y de la finalidad que persigue dicho acceso y/o comunicación -que podrá ser con los fines expresados en el propio artículo 1 de la LO 7/2021, como con otros fines en

función de la competencia del órgano o autoridad administrativa de que se trate-.

Finalmente como paso previo del análisis de las modificaciones y en la medida que el acceso al SIRAJ supone *per se* cesiones de datos o comunicaciones de datos es preciso recordar la doctrina del Tribunal Constitucional que es contraria las cesiones masivas de datos, por todas en Sentencia 17/2013, de 31 de enero de 2013, y que ha sido recogida en multitud de informes de esta Agencia, de cuyo contenido se desprende 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 (...).

IV

La primera modificación objeto de análisis es la referida al artículo 6 en sus apartados e), f) y g) que pretende dar acceso al SIRAJ y en concreto al Registro Central de Penados y en el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes a (e) las Policías Locales de los municipios con una población superior a los 250.000 habitantes o de más de 175.000 habitantes en el caso de las capitales de provincia, con carácter general, a través de los funcionarios autorizados, a la información contenida en el Registro Central de Penados y en el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes; (f) a las Fuerzas y Cuerpos de Seguridad dependientes de las Comunidades Autónomas, a través de los funcionarios autorizados; y también (g) al resto de Policías Locales y Autonómicas cuando las necesidades del servicio y las circunstancias concurrentes lo aconsejen y que lo soliciten de manera motivada.

También se añade un tercer apartado con la finalidad de que (iv) la persona encargada del Registro Central de Penados, siempre que se encuentren habilitados a tal efecto mediante una norma con rango de ley, proporcionará a los Organismos Públicos, por los medios electrónicos adecuados a tal fin, la

información que conste en dicho Registro y que resulte necesaria para la tramitación de sus procedimientos administrativos.

Pues bien, el artículo 5 del RGPD recoge los principios del tratamiento, entre los que cabe citar aquí los de licitud, minimización y limitación de la finalidad, según los cuales los datos personales serán:

- a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
- b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; (...) («limitación de la finalidad»);
- c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

Los “nuevos accesos” que se habilitan como consecuencia de la modificación han de ser respetuosos con los principios indicados, por cuanto deberán servir para el ejercicio de las competencias que, a estos actores les atribuya la ley (principio de licitud, artículo 6.1 e) RGPD y en su caso apartado c)) y para cumplir una finalidad que precisamente descansa en el ejercicio de dicha competencia y función (principio de finalidad) y únicamente acceder a datos personales en la medida que sean necesarios para cumplir la citada finalidad (principio de minimización).

La nueva redacción del precepto respecto de los accesos de las policías locales y autonómicas (letras e) y f)) hace la oportuna remisión al artículo 29.2 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad que dispone que *Para el cumplimiento de dicha función (judicial) tendrán carácter colaborador de las Fuerzas y Cuerpos de Seguridad del Estado el personal de Policía de las Comunidades Autónomas y de las Corporaciones Locales.*

Por tanto, las modificaciones de las letras e) y f) se alinean con los principios indicados valorándose favorablemente por esta Agencia.

En cuanto al apartado g), se deduce que se pretende permitir el acceso “al resto” de policías locales o autonómicas no incluidos en los anteriores, es decir, podrían estar integrados en este grupo bien porque no cumplan funciones de policía judicial (ex art. 29.2 LO 2/1986), bien porque, en el caso de las policías locales, la población de sus localidades no alcanza lo establecido en el

apartado e) anterior, y ello refiriéndose de una manera inconcreta a “necesidades del servicio y las circunstancias concurrentes lo aconsejen y que lo soliciten de manera motivada”.

La redacción de este apartado g), como se ha mencionado, adolece de una cierta inconcreción, y no se advierte, al no estar establecida en una ley (ya que esta norma es simplemente un Decreto), la necesidad de una finalidad adicional a la establecida en los apartados e) y f) anteriores, restringidas a la finalidad de dichos cuerpos policiales a una colaboración con los jueces y tribunales y el ministerio fiscal en labores de policía judicial, como resulta del art. 29.2 LO 2/1986, citada como razón de ser de ambos apartados e) y f). Por lo tanto, la redacción del apartado g) ha de ser congruente con los apartados e) y f) y exclusivamente para dichas funciones, sin que se considere conforme (STC 292/2000) una redacción abierta como la propuesta que deja al interesado sin conocer exactamente cuándo o para qué finalidades sus datos personales van a poder ser tratados, y al albur de una mera decisión administrativa. Lo contrario necesitaría una norma con rango de ley que estableciera, de manera precisa y conforme a los requisitos de la Constitución, el RGPD y la LOPDGDD, sin dejar al mero arbitrario de la autoridad administrativa el acceso de la Administración a los datos personales de los interesados. Corresponderá al legislador determinar los requisitos, circunstancias y situaciones en las que podrán tratarse (cederse) datos personales para finalidades diferentes de las propias a la que van dirigidos los tratamientos de los Registros a que se refiere el proyecto presentado a informe, sin que exista en la MAIN explicación acerca de la ley que permitiría estos tratamientos, regulándolos de manera que cumplan los parámetros que el Tribunal Constitucional ha entendido que han de cumplir las normas legales que prevén tratamientos.

Por tanto, se informa desfavorablemente al apartado g) del precepto.

En lo que se refiere a la letra h) del proyecto, que tiene por objeto dar acceso a la Administración Penitenciaria a través de funcionarios autorizados *en el ejercicio de las funciones de clasificación y programación del tratamiento de los internos que la legislación penitenciaria atribuye a los Servicios y Unidades de los Centros Penitenciarios de conformidad al artículo 281.1 del Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario*, debe indicarse que el art. 281 del Reglamento Penitenciario (no, como se dice en el proyecto, del RD 190/1996, que lo aprueba) no contiene una diferenciación en apartados ni parece regular *funciones de clasificación y programación del tratamiento de los internos* sino que hace referencia a los

“Subdirectores”. No se expresa por tanto parecer a este respecto. Por otra parte, en vez de hacer referencia a una norma reglamentaria, se considera que debería de hacerse referencia a la norma legal en la legislación penitenciaria que sustentaría dicho tratamiento de datos personales.

Y respecto del apartado 3 del artículo 6 que tiene por finalidad la comunicación a Organismos Públicos por medios electrónicos de la información que obre en el Registro Central de Penados, debe indicarse que es conforme a los criterios expresados en el presente informe en la medida que se requiere la habilitación por norma con rango de ley de los destinatarios de la información. Se sugiere, sin embargo, (i) a efectos de claridad y congruencia de la frase, así como (ii) a evitar interpretaciones del término “organismos públicos” puesto que el art. 84 de la ley 40/2015 contiene una definición que no parece ser la querida, en general, en este precepto del proyecto que se informa, que el citado apartado 3 se modifique de la siguiente manera:

3. La persona encargada del Registro Central de Penados proporcionará a los Organismos Públicos y demás entidades regidas por el derecho administrativo, siempre que se encuentren habilitados a tal efecto mediante una norma con rango de ley, por los medios electrónicos adecuados a tal fin, la información que conste en dicho Registro y que resulte necesaria para la tramitación de sus procedimientos administrativos”.

V

En cuanto a la modificación del artículo 8, denominado “Información de carácter general contenida en los Registros Integrados en el Sistema”, esta se refiere a la inclusión en el apartado a) de la fecha del atestado en los datos identificativos del condenado para poder identificar el atestado de manera inequívoca. Y también en el apartado c), haciéndose una referencia a la indicación de la convivencia en los datos personales identificativos de la víctima.

Pues bien, se consideran modificaciones favorables conforme al principio de exactitud de los datos recogido en el artículo 5.1 d) del RGPD según el cual los

datos personales serán *exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.*

Especial atención, e informe desfavorable, merece la adición de la letra e) a cuyo tenor:

e) En general, todos aquellos datos cuya inscripción sea acordada mediante resolución dictada por la persona titular de la Secretaría General para la Innovación y Calidad del Servicio Público de Justicia.

Debe recordarse que el precepto tiene por objeto recoger la información de carácter general que debe contener los Registros Integrados en el Sistema, y que como todo tratamiento de datos, debe cumplir, entre otros, los principios de limitación de finalidad y de minimización antes citados, para lo que es esencial conocer la información que contienen dichos registros.

Pues bien, lo cierto es que al remitir a una resolución de un órgano administrativo, la posibilidad de incluir más datos, (esto es, de realizar tratamientos sobre datos personales no establecidos en una norma) confrontaría el contenido del derecho fundamental a la protección de datos personales (véase STC ya citada 292/2000, entre otras)

En consecuencia, se informa desfavorablemente el apartado e).

VI

En cuanto a la modificación del artículo 9, denominado “Información contenida en la inscripción de sentencias firmes”, en su letra l) se añade la inclusión de *“las prohibiciones, deberes y condiciones derivadas de la suspensión impuestas y, en especial, las que deban ser comunicadas a las Fuerzas y Cuerpos de Seguridad”*, lo que esta Agencia valora positivamente al alinearse con el cumplimiento del principio de exactitud, por cuanto añade información impuesta por la propia resolución judicial que condiciona el cumplimiento de la medida de suspensión que refleja el Registro.

VII

En cuanto a la modificación del artículo 26 denominado “Tutela de derechos”, la modificación se concreta en la eliminación de la referencia directa al artículo 18.2 de la derogada Ley Orgánica 15/1999, de 13 de diciembre y se sustituye por el siguiente texto:

De conformidad con lo dispuesto en la normativa vigente en materia de protección de datos de carácter personal, los interesados podrán recabar la tutela de la Agencia Española de Protección de Datos en relación con el ejercicio de sus derechos de acceso, rectificación o cancelación

Como se ha indicado antes, la normativa de protección de datos aplicable al SIRAJ será el RGPD y la LOPDGDD, sin perjuicio de que en determinadas situaciones sería de aplicación la LO 7/2021, ya que muchos registros que se integran en el SIRAJ provienen de bases de datos de los órganos jurisdiccionales que se nutren de información derivada de tratamientos de datos con los fines del artículo 1 de dicha Ley Orgánica.

En consecuencia, el ejercicio de derechos podría verse afectado por según que norma resulte de aplicación, ya sea el Capítulo III del RGPD o el Capítulo III de la LO 7/2021.

Por tanto, se considera positivo la referencia genérica a la “normativa vigente de protección de datos de carácter personal”.

No obstante lo anterior, se propone la eliminación de la mención específica a cada derecho, en coherencia con ambos regímenes jurídicos (RGPD y LO 7/2021) ya que se regulan otros derechos además de los de acceso, rectificación o cancelación (además este último no aparece como tal en la regulación de protección de datos, sino que se ha sustituido actualmente por “supresión”), como es el de información y el de limitación.

En consecuencia, se propone la siguiente redacción:

De conformidad con lo dispuesto en la normativa vigente en materia de protección de datos de carácter personal, los interesados podrán recabar la tutela de la Agencia Española de Protección de Datos en relación con el ejercicio de sus derechos.

VIII

La disposición adicional segunda denominada “Prestación del consentimiento” resulta redactada en los siguientes términos:

A efectos de lo dispuesto en los artículos 6 b) y c) y 7.1 b) y c) del presente real decreto, el acceso de las Unidades de Intervención de Armas y Explosivos de la Guardia Civil y de las Unidades del Cuerpo Nacional de Policía responsables de la expedición del pasaporte a la información contenida en las Bases de Datos del Sistema de registros administrativos de apoyo a la Administración de Justicia, requerirá el previo consentimiento del interesado, quien podrá manifestarlo en la propia solicitud, salvo que una norma con rango de ley lo exceptúe.

La redacción propuesta tan sólo añade el inciso final (“salvo que una norma con rango de ley lo exceptúe”) a lo que ya disponía la citada disposición en su redacción original de 2009.

Debe acudirse en primer lugar a lo indicado en los citados preceptos (con la redacción por otra parte que da el proyecto que se informa). El artículo 6 apartados b) y c) determina lo siguiente:

Artículo 6. Acceso a la información contenida en el Registro Central de Penados y en el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes.

(...) el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes autorizará, (...) el acceso directo a la información contenida en el Registro Central de Penados y en el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes, (...) a:

b) Las unidades de Intervención de Armas y Explosivos de la Guardia Civil responsables de la concesión de los permisos de armas, a través de los funcionarios autorizados en relación con los fines que tienen encomendados.

c) Las unidades del Cuerpo Nacional de Policía responsables de la expedición del pasaporte, a través de los funcionarios autorizados en relación con los fines que tienen encomendados.

El art. 7.1.b) y c) establece la misma regulación para el acceso de estos funcionarios, en los mismos casos, al Registro Central de Protección a las Víctimas de la Violencia Doméstica y de Género.

La disposición adicional objeto de análisis, continuando con la redacción originaria del precepto en el RD 95/2009, propone el uso del *consentimiento* como fórmula jurídica que permita a las distintas unidades citadas acceder a los citados registros, (salvo que una norma con rango de ley lo exceptúe).

Pues bien, esta propuesta debe considerarse hoy día, al menos formalmente, p no conforme con el marco jurídico actual en materia de protección de datos por cuanto la base jurídica que legitimaría el tratamiento de dichos datos personales por las autoridades públicas es, con carácter general, el artículo 6.1 e) del RGPD (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); y en su caso, como parece que indica la norma proyectada como excepción, el apartado c) de dicho artículo (el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento); y no el consentimiento, que se considera residual en el ámbito de las autoridades públicas y su uso se limita a los casos en los que este expresamente previsto en la norma.

Así sucede, por ejemplo en la normativa tributaria en el artículo 95 k) de la Ley 58/2003, de 17 de diciembre, General Tributaria, o en el ámbito de los derechos de las personas con discapacidad en el artículo 38.2 Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, o como se va a analizar posteriormente en determinados casos, para acceder al Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos.

Las Unidades de Policía Nacional y de la Guardia Civil a las que hace referencia el precepto y la disposición adicional objeto de análisis, encuentran la legitimación de su acceso en los artículos 12 y 28 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, a cuyo tenor:

Artículo 12. Competencias sobre el pasaporte.

1. La competencia para su expedición corresponde:

a) En el territorio nacional, a la Dirección General de la Policía.

(...)

3. Corresponde al Gobierno, a propuesta de los Ministros del Interior y de Asuntos Exteriores y de Cooperación, desarrollar esta Ley en lo referente al régimen jurídico del pasaporte.

Artículo 28. Control administrativo sobre armas, explosivos, cartuchería y artículos pirotécnicos.

2. La intervención de armas, explosivos, cartuchería y artículos pirotécnicos corresponde al Ministerio del Interior, que la ejerce a través de la Dirección General de la Guardia Civil, cuyos servicios están habilitados para realizar en cualquier momento las inspecciones y comprobaciones que sean necesarias en los espacios que estén destinados a su fabricación, depósito, comercialización o utilización.

Resulta especialmente clarificadora con esta propuesta la disposición adicional octava de la LOPDGDD, denominada “*potestad de verificación de las Administraciones Públicas*”, por cuanto recoge, aunque no expresamente, la aplicación del artículo 6.1 e) RGPD a la actuación de las AAPP, ya que dispone lo siguiente:

Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

Y el propio artículo 28.2 de la de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (modificado por la LOPDGDD que sustituyó el consentimiento del interesado por la posibilidad de oposición del mismo, sobre la base de que la administración tiene potestad de verificación *cuando esos datos hubiera de aportarlos el interesado*, para facilitarle la tramitación administrativa al interesado, salvo que exista oposición de este a que la Administración lo compruebe, en cuyo caso corresponde a este su aportación) que dispone que

2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del

documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

En el presente caso, la lectura de los artículos 12 y 28 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, resulta coherente con la competencia que se otorga al Cuerpo Nacional de Policía y a la Guardia Civil, el acceso al Registro Central de Penados, al Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes, y al Registro Central de Protección a las Víctimas de la Violencia Doméstica y de Género para el ejercicio de dichas competencias, ya que de su contenido podrían resultar circunstancias que impidan emitir el pasaporte o el permiso de armas solicitado. Dicha comprobación ha de ser independiente, por razones obvias de interés público, de que el interesado declare, o no, tener alguna antecedente inscrito en dichos registros, puesto que la expedición del permiso de armas, o del pasaporte, requiere la comprobación de los datos que puedan establecer la posibilidad de emitir el documento solicitado, sin perjuicio, ciertamente, de que dicho acceso por el funcionario correspondiente está condicionado por la solicitud del permiso de armas o del pasaporte por el interesado.

En definitiva, la base jurídica del tratamiento de estos datos por el funcionario encargado será el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (art. 6.1.e) RGPD), y no el consentimiento.

El Tribunal Supremo, si bien bajo el régimen de vigencia de la anterior LOPD 1999, en sentencia de la Sala Tercera, de lo Contencioso-administrativo, Sección 5ª, Sentencia 1364/2021 de 23 de noviembre de 2021, Rec. 7919/2020, ha interpretado el art. 6 y 16 del RD 95/2009 y la normativa de protección de datos, en cuanto un funcionario policial accedió directamente al Registro de Penados para la comprobación de la habilitación de un guardia de seguridad, basándose la licitud del tratamiento en el interés público. Así:

*El control efectivo de los requisitos necesarios para mantener la habilitación para prestar servicio como vigilante de seguridad, como garantía del correcto desempeño de su función en el ámbito eminentemente público de la seguridad ciudadana, entre los que cobra especial relevancia el de carecer de antecedentes penales, deviene así **obligado** en el ejercicio por el poder público de su función esencial de garantizar la seguridad de los ciudadanos, en definitiva, de garantizar la convivencia y proteger el libre ejercicio de los derechos y libertades.*

Y el acceso al Registro Central de Penados y Rebeldes con esa finalidad resulta, asimismo, imprescindible para controlar este requisito de carecer de antecedentes penales y lograr así la finalidad última que se trata de salvaguardar, que la colaboración de los particulares en el ejercicio de esta función esencialmente pública se desarrolle con todas las garantías legalmente exigidas.

*Por tanto, debemos concluir que **el acceso al Registro Central de Penados y Rebeldes por parte de un funcionario de la Policía Nacional en el ejercicio de sus funciones, sin consentimiento del interesado, limitado a la comprobación del mantenimiento de un requisito necesario para la pervivencia de la habilitación para prestar servicios como vigilante de seguridad, carecer de antecedentes penales por delito doloso, está amparado** por el art. 11.2.c) LOPD 1999, en cuanto responde a **la libre y legítima aceptación de una relación jurídica** cuyo desarrollo, cumplimiento y control implica necesariamente la conexión con aquel fichero de terceros, el Registro Central de Penados y Rebeldes, siendo, por tanto, una cesión legítima de datos personales **que se encuentra legalmente prevista**, responde a una finalidad constitucionalmente legítima y es proporcionada a la salvaguarda de la misma.*

En consecuencia, y aunque esta AEPD comprende el propósito del legislador de incluir en la nueva redacción del precepto la excepción de la existencia de una ley a la necesidad del consentimiento del interesado, en realidad, dado que el consentimiento no es la base jurídica del tratamiento, dicha excepción no es necesaria. Por otro lado, la licitud de tratamiento de los datos personales (esto es, el acceso a los Registros) por los funcionarios que expidan pasaportes o permisos de armas vendrá determinada por el interés general, *establecido en una ley*, de la finalidad y necesidad de dicho tratamiento con un fin constitucionalmente legítimo.

Por lo tanto, se considera que a la Disposición Adicional en cuestión debería dársele una redacción diferente, congruente con el principio indicado, o suprimirla.

IX

Cuestión distinta al caso anterior, es la relativa a la disposición adicional quinta de la norma objeto de modificación.

Dicha norma proyectada tiene la siguiente redacción:

“Disposición adicional quinta. Uso de la Plataforma de Intermediación de Datos por parte de las Administraciones Públicas.

Las Administraciones y entidades competentes, previo consentimiento expreso del interesado, deberán obtener la certificación negativa del Registro Central de Penados y del Registro Central de Delincuentes Sexuales y Trata de Seres Humanos a través de la Plataforma de Intermediación de Datos de la Secretaría General de Administración Digital o por los medios electrónicos habilitados al efecto, cuando la ausencia de antecedentes penales o por delitos de naturaleza sexual o de trata de seres humanos constituya un requisito para el acceso a un derecho o adquirir una condición determinada, así como para ejercer profesiones, actividades u oficios que conlleven un contacto directo y habitual con personas menores de edad.”

El art. 3.2 del RD 1110/2015 establece las finalidades de dicho Registro, y en lo que aquí interesa el apartado 1 del mismo dice: *La finalidad del Registro es contribuir a la protección de las personas menores de edad contra la explotación y las agresiones sexuales, con independencia de quién sea el autor del delito, mediante el establecimiento de un mecanismo de prevención que permita conocer si **quienes pretenden el acceso y ejercicio** de profesiones, oficios y actividades que impliquen el contacto habitual con personas menores de edad, carecen o no de condenas penales por los delitos a los que se refiere el apartado anterior*

Lo que es coherente con el art. 57 de la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia, en el inciso final del apartado 1, que dice:

*(...) **quien pretenda** el acceso a tales profesiones, oficios o actividades **deberá acreditar** esta circunstancia mediante la aportación de una certificación negativa del Registro Central de delincuentes sexuales*

Parte por tanto la ley de la premisa de que se trata siempre de una petición de alguien que desea trabajar con menores, y para eso dicha persona pone en

marcha un procedimiento dirigido a (i) solicitar una certificación negativa del Registro Central de delincuentes sexuales, y (ii) a aportar dicha certificación negativa al empleador correspondiente para demostrar dicha circunstancia.

La regulación proyectada es coherente con lo dispuesto en la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia y en el Real Decreto 1110/2015, de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales (hoy día Real Decreto 1110/2015, de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos", según establece el art. único.1 del Real Decreto 407/2024, de 23 de abril), que requiere que la certificación (i) se expida a instancia del interesado y por tanto (ii) con el consentimiento de este, que acoge el criterio de esta Agencia expresado en varios informes.

Sirva citar el más reciente Informe 26/2023 sobre la adecuación al principio de proporcionalidad, de que sea el interesado quien deba aportar del certificado y, por tanto, que sea con su consentimiento y no basado en la voluntad de un tercero empleador lo que sustente el acceso a dicha información:

Partiendo de la anterior doctrina constitucional, en el caso de que lo que se pretendiera fuera la verificación de la ausencia de condenas penales directamente por el empleador o la organización dedicada a labores de voluntariado, dicho tratamiento de datos personales debe considerarse excesivo, al existir otras posibilidades menos lesivas para el derecho fundamental a la protección de datos como es la aportación de la certificación por el propio trabajador o voluntario, ratificándose esta Agencia en el criterio manifestado en su informe de 25 de julio de 2014

(...)

De este modo, mediando el previo consentimiento del interesado, se garantiza que el mismo conserve el poder de control y disposición sobre sus propios datos personales que le garantiza su derecho fundamental a la protección de datos (conforme a la doctrina sobre el alcance de este derecho fundamental recogida en la Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre, FJ.6).

Esta previsión es, asimismo, conforme con la regulación contenida en la Directiva 2011/93/UE del Parlamento Europeo y del Consejo de 13 de

diciembre de 2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, cuyo artículo 10.2 contempla tanto la previa autorización del interesado como la aportación por el mismo

(...)

En efecto, en el artículo 57 de la citada Ley Orgánica denominado “Requisito para el acceso a profesiones, oficios y actividades que impliquen contacto habitual con personas menores de edad” consta en su apartado 1 que:

*1. Será requisito para el acceso y ejercicio de cualesquiera profesiones, oficios y actividades que impliquen contacto habitual con personas menores de edad, el no haber sido condenado por sentencia firme por cualquier delito contra la libertad e indemnidad sexuales tipificados en el título VIII de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, así como por cualquier delito de trata de seres humanos tipificado en el título VII bis del Código Penal. A tal efecto, quien pretenda el acceso a tales profesiones, oficios o actividades deberá acreditar esta circunstancia mediante la **aportación de una certificación negativa** del Registro Central de delincuentes sexuales*

(...)

Y en el artículo 9 del Real Decreto 1110/2015, de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales denominado “Certificación de los datos inscritos” apartados 2 y 3 consta que:

2. La persona encargada del Registro, siempre que no se trate de información reservada a Jueces y Tribunales, y previo consentimiento expreso de la persona interesada o de su representante, informará de los datos relativos a la misma contenidos en el Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos, a instancia de cualquier órgano de las Administraciones Públicas o Colegio profesional ante el que se tramite un procedimiento para acceder a profesiones, oficios o actividades que impliquen un contacto habitual con personas menores de edad, así como para su ejercicio. En ausencia de tal consentimiento, el certificado se expedirá a instancia de la persona interesada en los términos previstos en el apartado siguiente.

Asimismo, las empresas y entidades, incluidas las de voluntariado, que den ocupación en cualesquiera profesiones, oficios y actividades que impliquen contacto habitual con personas menores de edad, podrán, previo consentimiento expreso de la persona interesada o de su representante, comprobar la inexistencia de antecedentes en el Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos, mediante la obtención de una certificación negativa del Registro, cuando sea necesaria para la contratación y ejercicio de la relación laboral o actividad. En ausencia de consentimiento expreso previo que habilite a las empresas y entidades al acceso al Registro, el certificado sólo podrá expedirse a instancia de la propia persona interesada en los términos previstos en el apartado tercero de este artículo.

3. A petición de la persona titular interesada, podrán certificarse directamente los datos relativos a su persona y suscribir certificaciones negativas respecto a personas que no figuren inscritas. Tratándose de personas menores de dieciséis años o de personas necesitadas de apoyo en el ejercicio de su capacidad jurídica, la solicitud habrá de efectuarse por representante legal, guardador de hecho, curador o defensor judicial, según corresponda. (...)

En consecuencia, se informa favorablemente la redacción de la disposición adicional quinta de la norma objeto de informe, debiendo en todo caso interpretarse de la manera sostenida por esta Agencia en sus informes, esto es, que la solicitud de acceso al registro ha de venir precedida no sólo del consentimiento previo y expreso del interesado para la expedición de la certificación correspondiente en todo caso, sino de una necesidad derivada de la finalidad de que el interesado desea acceder a una profesión, oficio o actividades para las que se requiere contacto habitual con menores de edad (art. 57 LO 8/2021).

X

Otra cuestión que es preciso indicar, que si bien no consta en el proyecto de Real Decreto sometido a informe, se ha observado al analizar el vigente 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, cuyos artículos 14 y 15 dicen lo siguiente:

Artículo 14. Seguridad del sistema.

1. Se implantarán en el Sistema de registros administrativos de apoyo a la Administración de Justicia las medidas de seguridad que correspondan, de conformidad con el Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

De cada intento de acceso se guardará como mínimo la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

2. Las redes de comunicación electrónica gestionadas por las comunidades autónomas que den soporte a los órganos judiciales estarán conectadas con el Sistema de Registros Centrales, en un entorno integrado en red, que garantice la confidencialidad y autenticidad de dichas comunicaciones.

Artículo 15. Seguridad de los datos.

Se aplicarán a los datos de carácter personal contenidos en el Sistema de registros administrativos de apoyo a la Administración de Justicia las medidas de seguridad que correspondan, de conformidad con el Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Como puede observarse se hace referencia al Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que debe entenderse que ha quedado obsoleto, así como ha quedado derogada la LOPD de 1999 con la aprobación del RGPD y de la LOPDGDD.

Uno de los cambios más significativos del nuevo régimen que instaaura el RGPD es el modelo de cumplimiento basado en la responsabilidad proactiva, que

supone el tránsito de un sistema estático a un entorno dinámico de permanente adaptación.

Así mientras en el Real Decreto 1720/2007, de 21 de diciembre se recogía un régimen de seguridad basado en un sistema “checklist” según el tipo de datos a tratar, nivel básico, nivel medio y nivel alto, en la actualidad el régimen de cumplimiento basado en la responsabilidad proactiva exige un análisis previo del riesgo por parte del responsable del tratamiento y en función del resultado la adopción de las medidas de seguridad que más se adecuen al tratamiento que vaya a realizar.

Los preceptos del RGPD que han de tenerse en cuenta a la hora de abordar este nuevo régimen de responsabilidad proactiva son los siguientes:

El artículo 5 en su apartado 1 letra f) y en su apartado 2 disponen lo siguiente:

Los datos personales serán:

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

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

Los artículos 24, 25 y 32 del RGPD disponen lo siguiente:

Artículo 24 “Responsabilidad del responsable del tratamiento” en su apartado 1:

- 1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.*

Artículo 25 “Protección de datos desde el diseño y por defecto”

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

Artículo 32 “Seguridad del tratamiento”

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la seudonimización y el cifrado de datos personales;*
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Por su parte la LOPDGDD en su artículo 28 dispone lo siguiente:

Artículo 28. Obligaciones generales del responsable y encargado del tratamiento.

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Como puede observarse estos preceptos ofrecen elementos a tener en cuenta por el responsable del tratamiento a la hora de llevar a cabo la responsabilidad proactiva de la que es acreedora y que se deriva precisamente de dicha condición de responsable del tratamiento.

Son medidas de carácter no exhaustivo y elementos a tener en cuenta en función del tipo de tratamiento, de ahí que se conciba la seguridad del tratamiento como un entorno dinámico en permanente adaptación y por tanto quede superado el régimen de seguridad de los datos basado en una lista estática de medidas en función de los datos a tratar tal como el que recoge el RD analizado al remitirse al Real Decreto 1720/2007, de 21 de diciembre por el

que se aprueba el Reglamento de desarrollo de la ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En definitiva, es esencial un análisis de riesgos previo al tratamiento, teniendo en cuenta múltiples elementos, y la adopción de medidas de seguridad será la consecuencia del resultado de dicho análisis, sin perjuicio de la necesidad de realización de la evaluación de impacto previsto en el artículo 35 del RGPD a cuyo tenor:

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

(...)

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

(...)

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

(...)

Por lo tanto, las referencias al Real Decreto 1720/2007 y la LOPD del año 1999 están fuera de lugar, por la derogación expresa de la LOPD y por el nuevo régimen de responsabilidad basado en la responsabilidad proactiva que supone la inoperatividad del sistema de seguridad basado en el citado Real Decreto.

Por último, citar que el SIRAJ en tanto sistema (informático) de información que trata datos de carácter personal **debe cumplir el ENS** y realizar la evaluación de impacto de acuerdo con el artículo 3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

Artículo 3. Sistemas de información que traten datos personales.

- 1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto 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) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, (...) así como los criterios que se establezcan por la Agencia Española de Protección de Datos (...) sin perjuicio de los requisitos establecidos en el presente real decreto.*
- 2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.*
- 3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.*