

**I**

El Anteproyecto de ley mencionado (en adelante APL) viene acompañado de la correspondiente Memoria de Análisis de Impacto Normativo (MAIN). Tal y como resulta de la Exposición de Motivos del APL, el objeto de la norma es, en esencia, la transposición de Directiva 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo. Esta norma encuentra su razón de ser en las crecientes interdependencias entre infraestructuras y sectores de prestación de servicios que utilizan infraestructuras clave en toda la Unión como la energía, el transporte, la banca, el agua potable, las aguas residuales, la producción, transformación y distribución de productos alimentarios, la sanidad, el espacio, la infraestructura de los mercados financieros y la infraestructura digital, y en ciertos aspectos del sector de la Administración pública. El APL expone que debido al carácter cada vez más interconectado y transfronterizo de las operaciones que utilizan infraestructuras críticas, las medidas de protección relativas únicamente a activos individuales no bastan y por tanto resulta necesario modificar el enfoque para garantizar que se tuvieran en cuenta todos los riesgos, se mejorase la definición y la coherencia de las funciones y las obligaciones de las entidades críticas que presten servicios esenciales para el funcionamiento del mercado interior de la Unión Europea, y se adaptasen sus normas a fin de aumentar la resiliencia de las entidades críticas

Desde la perspectiva de la normativa de protección de datos personales, que es lo que a esta AEPD le incumbe en este informe, la Directiva contiene unas menciones específicas en materia de protección de datos, que los Estado miembros deberán tener en cuenta a la hora de transponer dicha norma.

En primer lugar, el art. 1, apartado 9, de la Directiva 2022/2557 establece:

*La presente Directiva se entiende sin perjuicio del Derecho de la Unión en materia de protección de datos personales, en particular el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo.*

Es decir, la normativa de protección de datos personales (RGPD, Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas) etc. no se ven exceptuadas, por lo que los tratamientos de datos personales, cuando existan, habrán de cumplir con estas normas.

En segundo lugar, la Directiva establece específicos tratamientos de datos personales, requeridos por el especial propósito de la norma, entre los que cabe destacar en el art. 14 la comprobación de antecedentes personales de aquellas personas que, con carácter general, vayan a desempeñar algunas funciones determinadas en una entidad crítica. Dichos antecedentes personales deberán incluir los antecedentes penales (Considerando 32 de la Directiva).

En cualquier caso, el art. 14.2 de esta norma deja a salvo la normativa de protección de datos, y específicamente establece:

*Las solicitudes a que se refiere el apartado 1 del presente artículo se evaluarán en un plazo razonable y se tramitarán de conformidad con el Derecho y los procedimientos nacionales y con el Derecho de la Unión pertinente y aplicable, incluidos el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo. Estas comprobaciones de antecedentes serán proporcionadas y se limitarán estrictamente a lo necesario. Se realizarán con el único fin de evaluar un posible riesgo para la seguridad de la entidad crítica de que se trate.*

En lo que a este informe concierne, pues, la Directiva explicita que el examen de dichos antecedentes personales habrá de llevarse a cabo de acuerdo con el derecho aplicable, y cita ambas normas, el RGPD y la Directiva 2016/680, con lo que no se pronuncia sobre cuál ha de ser la norma que regula estos tratamientos, lo que dependerá, por tanto, de si los tratamientos de datos personales los llevan a cabo 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 (art. 1 Ley Orgánica 7/2021), o aunque los tratamientos de datos los lleven a cabo dichas autoridades sus finalidades son distintas de las mencionadas, en cuyo caso será de aplicación el RGPD (art. 2.3.a) LO 7/2021).

## II

Conviene recordar cuál es la doctrina tanto de los tribunales españoles como del TJUE cuando los tratamientos de datos personales pueden comprender datos especialmente protegidos.

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

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

*Y ello porque, en el ámbito de las categorías especiales de datos personales, (...) el Reglamento general de protección de datos establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales. **En cambio, no establece por sí mismo el régimen jurídico aplicable a los tratamientos de datos personales especiales**, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión. Por ende, tampoco fija las garantías que deben observar los diversos tratamientos posibles de datos sensibles, adecuadas a los riesgos de diversa probabilidad y gravedad que existan en cada caso; tratamientos y categorías especiales de datos que son, o pueden ser, muy diversos entre sí. El Reglamento se limita a contemplar la posibilidad de que el legislador de la Unión Europea o el de los Estados miembros, cada uno en su ámbito de competencias, prevean y regulen tales tratamientos, y a indicar las pautas que deben observar en su regulación. Una de esas pautas es que **el Derecho del Estado miembro establezca «medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado»** [artículo 9.2.g) RGPD] y que «se ofrezcan garantías adecuadas» (considerando 56 RGPD). **Es patente que ese establecimiento de medidas adecuadas y específicas solo puede ser expreso**. Si la norma interna que regula el tratamiento de datos personales relativos a opiniones políticas no prevé esas garantías adecuadas, sino que, todo lo más, se remite implícitamente a las garantías generales contenidas en el Reglamento general de protección*

*de datos, no puede considerarse que haya llevado a cabo la tarea normativa que aquel le exige.*

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].*

Vistos ya sucintamente las previsiones de la directiva a trasponer, y las previsiones de los tribunales (TC y TJUE) sobre las leyes que han de contener injerencias en el derecho fundamental a la protección de datos cuando se tratan datos especialmente protegidos, pasamos al contenido del APL.

### III

El art. 9 APL regula la comprobación de “la idoneidad” de personas. En sí mismo, el título del artículo no sería completo, por cuanto como resulta del Considerando 32 de la Directiva, cabe distinguir entre comprobación de la identidad y de la idoneidad, y ambos han de llevarse a cabo.

El apartado 1 del art. 9 señala que “La Secretaría de Estado de Seguridad especificará, en los términos que se determinen reglamentariamente, las condiciones en las cuales, en casos debidamente motivados y teniendo en cuenta la Evaluación Nacional de Amenazas y

Riesgos, se permita a una entidad crítica presentar solicitudes de comprobación de los antecedentes personales *a través del tratamiento de datos personales al que se refiere la disposición adicional quinta (...)*. Realiza por tanto una remisión a la DA 5ª APL. No obstante, el apartado 2 de este art. 9 añade, al final, que dichas solicitudes “*se tramitarán de conformidad con el ordenamiento jurídico*”.

Sin perjuicio de señalar que dicha mención al ordenamiento jurídico es una apelación vacía de contenido, y por tanto innecesaria (pues las solicitudes no se pueden tramitar de una manera que no sea conforme al ordenamiento jurídico), esta AEPD desea señalar que parece contradictorio, o incongruente, que en el apartado 1 se dirija el procedimiento a la DA 5ª del APL y en el apartado 2 se establezca que su tramitación será conforme al ordenamiento jurídico. De ello resulta que esta AEPD desconoce si es que se desea que la tramitación de las solicitudes de comprobación de antecedentes personales por las entidades críticas se lleve a cabo según la legislación sectorial en cada caso aplicable -si esta legislación sectorial contuviese en cada caso, lo que se desconoce, una regulación expresa a tal fin, o bien se pretende en el APL una sola tramitación, con normativa única, para todas las entidades críticas, con independencia del sector en que actúen. Se sugiere que por el prelegislador se especifique y se redacte de nuevo para aclarar esta posible inconcreción.

El apartado 3 establece que la comprobación de los antecedentes personales será proporcionada etc. e incluirá como mínimo, las siguientes actuaciones.

Tal y como hemos expuesto en el epígrafe II (STC 76/2019), es *la misma ley* la que «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».

En consecuencia, si bien la Directiva establece la mención “como mínimo” (art. 14.3) para las actuaciones a llevar a cabo para comprobar la identidad e idoneidad, la ley de transposición ha de concretar, ella misma, las actuaciones a llevar a cabo en comprobación de la identidad e idoneidad, sin que ese “como mínimo”, al quedar a la discreción de la autoridad administrativa y poder, por tanto, sin más limitaciones, incluir el tratamiento de cualquier tipo de datos personales, pueda considerarse que cumple las condiciones y requisitos exigidos por la jurisprudencia. Será la ley la que habrá de determinar “ella misma” cuáles son los datos personales que este tratamiento podrá incluir. Por lo tanto, se informa desfavorablemente a dicha mención.

#### IV



La Disposición adicional tercera (DA 3ª) hace referencia a la Protección de datos de carácter personal.

Como ya se ha expuesto, la Directiva que la ley traspone no contiene un régimen específico de protección de datos, sino que se remite, y por tanto ha de cumplirse, el régimen general de protección de datos que resulte aplicable (art. 1.9)

Ahora bien, a diferencia de la Directiva, que es una norma para trasponer en el derecho del Estado miembro, la ley nacional debería de establecer con claridad los distintos tratamientos de datos que resulten de la propia ley, y establecer ella misma cuáles son esos tratamientos y en consecuencia cuáles se regulan conforme a unas disposiciones y cuáles conforme a otras.

Esta AEPD no puede considerar favorablemente una disposición como el apartado 1 de la DA 3ª, pues de la misma no resulta ni los tratamientos que surgen de esta ley ni su regulación. Se mezclan, sin distinción, regulaciones dispares y con consecuencias y requisitos igualmente distintos, lo que impide a los interesados una visión clara, o un conocimiento adecuado, de los tratamientos que resultan de la norma. En definitiva, este apartado tan sólo conduce a la confusión, por cuanto no aclara o distingue tratamientos, sino que se mezclan las regulaciones sin aclarar.

Cabe en este punto añadir que no se ha aportado con el expediente presentado a esta AEPD análisis de riesgo, Evaluación de Impacto en materia de protección de datos (EIPD) o informe del Delegado de protección de datos del órgano administrativo redactor del proyecto, que puedan arrojar alguna luz tanto acerca de los tratamientos que puedan surgir de esta ley, como de la regulación aplicable a cada uno de ellos. Esta AEPD lo desconoce, y de lo que parece de la redacción del precepto, tampoco el anteproyecto presentado lo solventa adecuadamente, limitándose en la redacción a acumular (como veremos posteriormente además en la DA 5ª) normativas que permitan, sin una distinción clara, acoger todos los supuestos, como para evitar que se escape alguno, pero sin estructurar estos.

En el apartado 2 de esta DA 3ª se dice que [l]a Secretaría de Estado de Seguridad podrá tratar los datos que le sean comunicados por las entidades críticas designadas, [...] y que resulten necesarios para el cumplimiento de las disposiciones de esta ley y *otra normativa con incidencia en la resiliencia de entidades críticas*. Esta AEPD cree conveniente reiterar una vez más que esta pretendida utilización de los datos personales para finalidades diferentes de las previstas inicialmente (que son el cumplimiento de las finalidades de esta ley, que se denomina de resiliencia de las entidades críticas) podría estar

justificada, pero para ello esta AEPD considera conveniente que se justifique por el prelegislador que norma autoriza dichos tratamientos para finalidades diferentes de las iniciales: bien el art. 6.4 RGPD bien el art. 6.2 de la LO 7/2021. Ello dependerá, por lo tanto, de cuál es la norma que se aplica a los tratamientos regulados en este APL: si el RGPD y la LOPDGDD o la LO 7/2021, cuestión esta no resuelta en el APL, y sobre el que no se arroja ninguna claridad.

Por otra parte, como puede observarse, existe una discordancia entre el apartado 3 de la DA 3ª, que sólo permite el tratamiento de datos personales comunicados para los fines previstos en esta ley y el apartado 2, que permite tratamientos para otros fines distintos de esta ley, pero eso sí, siempre que tengan incidencia en la resiliencia de las entidades críticas.

El apartado 4 regula, de una manera que esta AEPD considera desfavorablemente, restricciones a los derechos fundamentales a la protección de datos de los interesados. Al igual que se ha mencionado en los párrafos anteriores, luce en esta regulación un desconocimiento, o no se trasluce de esta regulación, de la normativa que efectivamente aplica a los tratamientos de datos que surgen de la norma que se informa.

Así, las posibles limitaciones a los derechos de los interesados que se regulen por el RGPD requieren que *la propia ley* (ver art. 23 RGPD) establezca, con carácter general, las restricciones específicas a los derechos de los artículos 12 a 22 RGPD, cuando tal limitación establecida por esa ley respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar ciertos valores que se explicitan en el art. 23.1 RGPD. Además, esa *ley* deberá contener, como mínimo, disposiciones específicas relativas a: la finalidad del tratamiento o de las categorías de tratamiento; las categorías de datos personales de que se trate; el alcance de las limitaciones establecidas; las garantías para evitar accesos o transferencias ilícitos o abusivos; o la determinación del responsable o de categorías de responsables. El APL sometido a informe no contiene ninguna de estas consideraciones, luego es de suponer que estas limitaciones no se aplicarán a los tratamientos que resulten estar regulados por el RGPD (los cuales, se reitera, no se sabe cuáles son por no venir especificados en el APL).

Los arts. 20 a 23 de la LO 7/2021 regulan, a su vez, los derechos de los interesados en los tratamientos que se regulan por dicha norma. Parece que la redacción del apartado 4 de la DA 3ª, *que limita exclusivamente el derecho de acceso*, estaría más inspirado en el art. 24 de la LO 7/2021, pero con una redacción que, en opinión de esta AEPD, tan sólo presentaría problemas de interpretación, tanto por el uso gramaticalmente cuando menos discutible de los gerundios como porque debiendo ser la redacción de la cláusula que limite los derechos de los interesados similar a la norma que lo rige (como es la LO



7/2021) se aparta de ella innecesariamente. Esta AEPD sugeriría que dicho apartado 4 se redacte bien remitiéndose al art. 24 de la LO 7/2021, bien redactándose de mane asimilar al citado art. 24. Por ejemplo, así:

*En los casos en que el tratamiento de datos personales esté regido por la Ley Orgánica 7/2021, de 26 de mayo, el responsable del tratamiento podrá denegar, total o parcialmente, las solicitudes de ejercicio del derecho de acceso del interesado a sus datos personales contemplado en el artículo 22 de dicha Ley Orgánica 7/2021, siempre que, teniendo en cuenta los derechos fundamentales y los intereses legítimos de la persona afectada, 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.*

*En lo no regulado en esta ley en este aspecto, se estará al resto del artículo 24 de la Ley Orgánica 7/2021, de 26 de mayo.*

En definitiva, se quiere reiterar aquí por esta AEPD que (i) las limitaciones al derecho fundamental a la protección de datos personales dependerán, para sus requisitos, de la norma que regula los tratamientos de datos personales de que se trate en cada caso (tal y como por otra parte se recoge en el propio apartado 1 de la DA 3ª APL) ya sea el RGPD/LOPDGDD ya sea la LO 7/2021; (ii) consecuencia de lo anterior es que no sería bastante la redacción del apartado 4 de la DA 3ª, por cuanto no cumpliría los requisitos del art. 23 RGPD -para los tratamientos regidos por el RGPD- ni tampoco, por separarse de él, los del art. 24 de la LO 7/2021 para aquellos tratamientos que se rijan por esta norma.

## **V**

La Disposición Adicional quinta (DA 5ª) regula los “*Informes y comprobaciones para acreditaciones y antecedentes (INCOA)*”

Tal y como resulta de la MAIN:

*El tratamiento de datos personales INCOA, es el tratamiento que instrumentaliza el ejercicio de las competencias de comprobación de antecedentes personales reconocidas, entre otras, en las siguientes normas: Ley de Enjuiciamiento Criminal, Reglamento sobre instalaciones nucleares y radiactivas, aprobado por el Real Decreto 1836/1999, de 3 de diciembre; Reglamento (CE) 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, por el que se establecen las normas comunes para la seguridad de la aviación civil; Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana; Ley Orgánica 7/2021, 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.*

*Asimismo, INCOA será el tratamiento de datos personales empleado para materializar la comprobación de los antecedentes personales, a la que se refiere el 9 del anteproyecto y que desarrolla el artículo 14 de la Directiva CER, de quienes realicen determinadas tareas en las entidades críticas.*

Esto es, parece que el prelegislador ha querido establecer, mediante esta norma, un único tratamiento de datos personales para las competencias que determinados órganos públicos puedan tener en algunas normas (ni siquiera cita todas (dice “entre otras”) para “comprobar antecedentes”, y ello sin una comprobación de que estas normas, todas ellas (incluso las no nombradas, requieren exactamente las mismas necesidades de comprobación de antecedentes, incluso “antecedentes penales”, ya que se trata de uno de los posibles datos personales que se podrán tratar en el ejercicio de este tratamiento de datos, como resulta de la norma. Dado que no se ha presentado análisis de riesgos ni EIPD, como ya se ha comentado, no es posible conocer si esos datos son necesarios, en qué medida, o qué medidas se han adoptado o son necesarias, según la EIPD, para mitigar los riesgos.

Por otra parte, aun cuando tampoco se ha aportado con el expediente a esta AEPD, resulta del Inventario de tratamiento del Ministerio del Interior que ya existe un tratamiento de datos personales denominado “*Informes y comprobaciones para acreditaciones (INCOA)*; Tratamiento bajo la Ley Orgánica 7/2021”, que coincide en lo esencial con el tratamiento que se regula en el APL sometido a informe, si bien, y es importante, este nuevo somete a tratamiento los “*antecedentes penales*”, que el citado en el Inventario no

incluía. Y demás, la base del tratamiento se establece como el “art. 11 de la Ley orgánica 7/2021”).

Entrando en la regulación en el APL de este tratamiento:

En el apartado 1 se establece como responsable del tratamiento a la Dirección General de Coordinación y Estudios de la Secretaría de Estado de Seguridad. En este aspecto, es de señalar que el art. 11.1 de la LO 7/2021 es clara en el sentido de que la licitud de los tratamientos de datos basados en los fines de esa norma requiere que estos sean necesarios para los fines del art. 1 de la LO 7/2021, pero además, también, que se realicen realice por una autoridad competente en ejercicio de sus funciones. Esto es, no es suficiente con que este artículo determine como responsable del tratamiento a la Dirección General citada, sino que esta ha de tener establecidas entre sus funciones, con claridad (art. 8 ley 40/2015: *La competencia es irrenunciable y se ejercerá por los órganos administrativos que la tengan atribuida como propia (...)*), la competencia para la cual el APL le reconoce ahora como responsable del tratamiento. No resulta del APL o la MAIN de donde provienen esas competencias, ni tampoco resultan del art. 6 del Real Decreto 207/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. La norma correspondiente deberá establecer claramente esta competencia específica en la Dirección General (esto es, la competencia para otorgar las acreditaciones en las distintas normas cuyo tratamiento de datos trata de regular, de manera conjunta, esta DA 5ª).

En el apartado 2, finalidades, no se comparte la redacción del APL. Los principios de claridad y proporcionalidad requerirían, en opinión de esta AEPD, que el prelegislador haga un ejercicio de exhaustividad en cuáles son las finalidades concretas de cada tratamiento de datos personales regulado por esta norma; esto es, en vez de realizar una redacción omnicomprendensiva, contraria al principio de calidad normativa y de claridad, la norma debería de especificar todos los tratamientos, uno a uno, respecto de los cuales se aplicará este tratamiento. No estima esta AEPD que ello sea un ejercicio difícil, pero aunque así fuera, las finalidades de los tratamientos no pueden estar redactados de manera ambigua, o vaga, como resulta del texto propuesto. En la MAIN se mencionan algunos textos legales cuyos tratamientos de datos personales se encauzarán por este precepto. Esta AEPD considera que deben especificarse todas las finalidades en este apartado, para que los interesados puedan conocer los concretos tratamientos de datos a los que se aplica este precepto.

El apartado 3 establece que:

*En el tratamiento informes y comprobaciones para acreditaciones y antecedentes, se podrán tratar, al menos, los datos relativos a la identidad de las personas, datos de contacto, dirección, residencia,*

*datos laborales, sus antecedentes penales y policiales, los datos personales de identidad y contacto de los responsables, gestores y usuarios del fichero del tratamiento.*

Esta AEPD no comparte esta redacción, y lo que conlleva: como ya hemos expuesto en el epígrafe II de este Informe, el Tribunal Constitucional ha expresado que:

*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).*

Esto es, la expresión “al menos” no es conforme a derecho, ya que implicaría dejar al albur de la autoridad administrativa los datos que van a ser tratados en estos tratamientos, lo que no sería admisible. Tienen que venir establecidos en la propia ley. No parece que haya habido ningún tipo de cuestión en este respecto, pues ya se recoge en el apartado correspondiente del Tratamiento INCOA en el Inventario de tratamientos del Ministerio del Interior, al que ya se ha hecho referencia, una lista exhaustiva (no abierta) de datos personales que podrán ser tratados en estos tratamientos.

El apartado 4 recoge quienes son los “destinatarios” de los datos, y cita *a los órganos jurisdiccionales del orden penal, el Ministerio Fiscal y las Fuerzas y Cuerpos de Seguridad, así como otras entidades únicamente cuando se prevea legalmente*. Esta AEPD considera que dicha lista, y la ausencia en ella de las entidades críticas, objeto fundamental de este APL, es consecuencia de la falta de concreción de las finalidades de cada tratamiento específico que se pretende aglutinar en este precepto. Esta AEPD considera que debería, al igual que ya se ha expuesto en el apartado 2 de esta DA, distinguirse o diferenciarse en cada caso los específicos tratamientos concretos, y en ellos establecer los destinatarios, determinando, por cada norma que ampare un tratamiento, los destinatarios de los datos personales. En concreto, y como ejemplo, no cabe considerar que, en todos los casos, los destinatarios sean “los órganos jurisdiccionales” pues un antecedente “positivo” de una persona cuyo examen de antecedentes haya sido solicitado por una entidad crítica (se reitera, finalidad principal de esta ley) tenga por destinatario a los órganos jurisdiccionales.

El art. 5 sirve para comprobar que no parece complejo determinar a qué normas o finalidades sirven estos tratamientos. Aquí sí se establecen los posibles destinatarios (también son destinatarios), por lo que esta AEPD considera que la redacción debería de distinguir entre cada tratamiento concreto y los destinatarios respecto de cada norma que regule el tratamiento de solicitud de antecedentes.

En el apartado 7 se están mezclando conceptos del RGPD con los de la LO 7/2021. De acuerdo con la LO 7/2021 (arts. 11 y 1), y como ya se ha mencionado, *El tratamiento sólo será lícito en la medida en que sea necesario para los **finés señalados en el artículo 1** y se realice por una autoridad competente en ejercicio de sus funciones*

Corresponde al prelegislador determinar si este tratamiento está dirigido a 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* (art. 1 LO 7/2021) o bien está dirigido, o tiene por objetivo o base de licitud, *el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*, pero diferentes a las ya citadas 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*. Según el caso, será aplicable el régimen del RGPD o de la LO 7/2021. **Cuestión esta, por otra parte, y dado que no se ha aportado informe del DPD con la documentación, de la que falta todo análisis por parte del prelegislador**, y que por supuesto, se extiende al régimen de protección de datos en todo el APL, y no sólo en este apartado.

En el apartado 12, se muestra conformidad con el primer párrafo, y no se comparte, y se estima que deberían suprimirse los tres párrafos finales del apartado.

Ya la LO 7/2021, régimen de tratamiento de datos en que se mueve este APL, contiene un régimen íntegro y completo de las restricciones o limitaciones al derecho fundamental a la protección de datos personales en este régimen. Los párrafos cuya supresión se propugna no son sólo confusos, sino contradictorios, o directamente contrarios a dicha regulación.

El párrafo segundo del apartado 12 de la DA 5ª establece un régimen contradictorio con el art. 26.1 LO 7/2021 al que dice referirse. Este art. 26.1 dice que cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales, el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento a los que se hace referencia en los artículos anteriores se llevará a cabo *de conformidad con las normas*

*procesales penales*. Como puede observarse, este art. 26.1 LO 7/2021, con rango por otra parte de **ley orgánica** (al igual que las normas procesales penales, Ley de Enjuiciamiento Criminal) no establece un régimen alternativo (“o”) que permita, directamente, al responsable del tratamiento restringir los derechos los derechos de acceso, rectificación, limitación y supresión respecto al tratamiento de datos en el fichero.

El párrafo tercero del apartado 12 de la DA 5ª, adolece, como todo el texto del APL en materia de tratamiento de datos, como ya se ha expuesto, de confusión entre los regímenes del RGPD y de la LO 7/2021. En concreto, este precepto establece un plazo para proporcionar información “de un mes prorrogable a otros dos”. Como puede observarse, el art. 20.4 LO 7/2021 establece para ello un plazo de un (1) mes. Es el RGPD, régimen que aquí no aplicaría, en su art. 12.3, el que establece la posibilidad de ampliar en dos meses el plazo inicial de un mes. El régimen de restricción del derecho fundamental de protección de datos se regula, de nuevo, se reitera, con carácter de ley orgánica, en el art. 24 LO 7/2021, cuyo apartado 2 ya regula la posibilidad para el responsable del tratamiento de que: *[l]as razones de la restricción podrán ser omitidas o ser sustituidas por una redacción neutra cuando la revelación de los motivos de la restricción pueda poner en riesgo los fines a los que se refiere el apartado anterior*.

En cuanto al último párrafo del apartado 12 de la DA 5ª, ya se regula en el art. 26.2 LO 7/2021, lo que lo hace innecesario, y además puede crear confusión acerca de a qué se refiere, por cuanto la redacción es diferente de la del art. 26.2 LO 7/2021.

Por estas razones se considera que deberían de suprimirse los párrafos segundo a cuarto de la DA 5ª, apartado 12, y referirse para el régimen de restricción de derechos a los arts. 20 a 26 de la LO 7/2021.

## **VI**

La DA 7ª del APL dice así:

*En virtud de lo dispuesto en el artículo 26 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, y teniendo en cuenta la Evaluación Nacional de Amenazas y Riesgos, las entidades críticas establecerán sistemas de reconocimiento biométrico de identificación o autenticación en todas o algunas de sus instalaciones con objeto de garantizar el control de accesos y el desplazamiento con fines de prevención de delitos y seguridad física. La implantación de estos sistemas, las características que deben reunir y su extensión, se regularán mediante orden del Ministro del Interior.*



Esto es, establece una obligación para las entidades críticas de establecer sistemas de reconocimiento biométricos.

Para comenzar con el análisis de este precepto, se establece un verdadero tratamiento de datos, pero a diferencia de los anteriores que hemos desglosado en este informe, los responsables de los tratamientos serán las propias “entidades críticas”, las cuales, en principio, no son “autoridades competentes” en el sentido del art. 4 de la LO 7/2021. Ello significa que estos tratamientos estarán sujetos al régimen del RGPD en toda su extensión (no al de la LO 7/2021).

El RGPD, art. 4.14), define «datos biométricos» como *datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*.

Las Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público (véase Versión 2.0, de 26 de abril de 2023), determinan, en su apartado 12, que el concepto de dato biométrico abarca tanto la “autenticación” como la “identificación”, y si bien son conceptos distintos, en ambos procedimientos se tratan datos dirigidos a identificar a una persona física, por lo que ambos se incluyen en el concepto de “tratamientos de datos”, y más específicamente, **son tratamientos de datos personales de categorías especiales**.

Cabe recordar, por otra parte, que el art. 9.1 RGPD establece que:

***Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.***

En consecuencia, a los datos biométricos (a ambos tipos) se extiende la **prohibición general establecida en el art. 9.1 del RGPD**, por lo que dicha prohibición ha de aplicar no sólo a los tratamientos dirigidos a la identificación sino también a los supuestos de tratamientos de datos biométricos dirigidos a la autenticación o verificación de la persona con respecto al patrón previamente establecido para la misma.

Es por lo tanto, necesario, en este momento traer a colación de nuevo la tan retirada Sentencia del Tribunal Constitucional 76/2019, que establece las

circunstancias a tener en cuenta cuando se establecen tratamientos de datos personales de categorías especiales, por cuanto la regulación contenida en el APL es insuficiente y no levantaría la prohibición del art. 9.1 RGPD.

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

Y ello porque, **en el ámbito de las categorías especiales de datos personales**, (...) el Reglamento general de protección de datos establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales. **En cambio, no establece por sí mismo el régimen jurídico aplicable a los tratamientos de datos personales especiales**, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión. Por ende, **tampoco fija las garantías** que deben observar los diversos tratamientos posibles de datos sensibles, adecuadas a los riesgos de diversa probabilidad y gravedad que existan en cada caso; tratamientos y categorías especiales de datos que son, o pueden ser, muy diversos entre sí. El Reglamento se limita a contemplar la posibilidad de que el legislador de la Unión Europea o el de los Estados miembros, cada uno en su ámbito de competencias, prevean y regulen tales tratamientos, y a indicar las pautas que deben observar en su regulación. Una de esas pautas es que **el Derecho del Estado miembro establezca «medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado»** [artículo 9.2.g) RGPD] y que «se ofrezcan garantías adecuadas» (considerando 56 RGPD). **Es patente que ese establecimiento de medidas adecuadas y específicas solo puede ser expreso**. Si la norma interna que regula el tratamiento de datos personales relativos a opiniones políticas no prevé esas garantías adecuadas, sino que, todo lo más, se remite implícitamente a las garantías generales contenidas en el Reglamento general de protección de datos, no puede considerarse que haya llevado a cabo la tarea normativa que aquel le exige.

(...)

*La cuestión solo puede tener una respuesta constitucional. **La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales** de que se trate. **Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento**, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del artículo 53.1 CE para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales.*

*Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas –unas veces– de predeterminación normativa y –otras– de **calidad de la ley** como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, **no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares.***

Ello significa, en concreto, que la regulación legal contemplada en el APL no es suficiente por no estar predeterminadas en ella no sólo las garantías del tratamiento, sino ni siquiera cuál es la causa de entre las establecidas en el art. 9.2 RGPD que levantaría la prohibición del tratamiento de los datos personales biométricos.

Esta AEPD considera, ciertamente, que puede ser razonable un tratamiento de datos biométricos para la protección de entidades críticas, y que ello podría encajar en el interés público esencial del art. 9.2.g) RGPD. Pero ello requiere la determinación por el legislador no sólo de esta circunstancia, fundamentándolo adecuadamente, sino asimismo la regulación completa del tratamiento de datos personales a que se refiere, sin remitirse a norma reglamentaria o decisión de autoridad administrativa o de los propios particulares. Es necesario, además, como expresamente requiere la jurisprudencia citada y el propio art. 9.2.g) RGPD, que esa ley *proporcional al*

*objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;*

La proporcionalidad del tratamiento debería de ponderarse en la correspondiente EIPD que se realizara (preferiblemente por el prelegislador, ex art. 35 RGPD), y en todo caso en la ley que se redacte deberían establecerse las medidas “adecuadas y específicas” para proteger los intereses y derechos fundamentales del interesado.

En definitiva, la DA 7ª sería contraria a la jurisprudencia expuesta, y por lo tanto al RGPD.

## **VII**

En el apartado 6.7 de la MAIN se hace referencia, en lo referente al “Impacto en materia de protección de datos personales, que “la norma tiene un “impacto positivo” (sic) en materia de protección de datos personales, “al regular la materia garantizando la protección de este derecho fundamental”.

Esta AEPD considera que dicha expresión es desafortunada por incorrecta, pues toda norma que establece (impone) un tratamiento de datos personales supone una afección al derecho fundamental a la protección de datos personales, que, como es sabido, el TC en su STC 292/2000 estableció que se concreta en un poder de disposición y de control sobre los datos personales. De esta manera, la persona debe quedar facultada para decidir cuáles de sus datos proporcionar a un tercero, sea la Administración o un particular, decidir cuáles puede este tercero recabar, saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Ahora bien, ese derecho fundamental no es absoluto, sino que habrá que ponderar su prevalencia o no en relación con otros derechos o intereses constitucionalmente protegidos. De ahí que el legislador europeo, en la Directiva tan citada, y el APL, hayan ponderado que un bien digno de protección, como la protección de las entidades críticas, amerite una afectación al derecho fundamental en los términos establecidos por la Directiva y el APL (teniendo en cuenta lo señalado en este Informe), pero ello no supone en ningún caso un “*impacto positivo*” en el derecho fundamental. La expresión usada en la MAIN parece confundir la afectación al derecho fundamental, que es el “*impacto*” cuyo análisis exige que se lleve a cabo en la MAIN, con las medidas que, en relación con las garantías de ese derecho, se establecen en la Directiva y el APL para paliar esa afectación (o impacto negativo) en el derecho fundamental.