

**0002/2023**

El Anteproyecto presentado a informe aborda la reforma de cuatro normas, cada una de ellas en un artículo del anteproyecto, todas ellas relacionadas con aspectos penales. A los efectos de la normativa de protección de datos personales ello supone que los tratamientos de datos que hayan de realizarse por las autoridades competentes en el ejercicio de dichas funciones penales habrán de regirse, en principio, por 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 (LO 7/2021), dictada en desarrollo de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (Directiva 2016/680).

En concreto, el art. 2.2 de la LO 7/2021 establece que *[e]l 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, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, las leyes procesales que le sean aplicables y, en su caso, por la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.*

El art. 1 de la LO 7/2021 señala que dicha ley tiene por objeto *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 el art. 4, después de establecer qué ha de entenderse por autoridades competentes a los efectos de esta norma, incluye dentro de su

ámbito a las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

I

El artículo primero del anteproyecto modifica Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ) para incluir en el art. 277 una regla subsidiaria de prestación de cooperación judicial en materia penal por razón de reciprocidad, cuando no exista tratado o convenio, normas de la UE o legislación española en la materia. Y el art. 278.1.5º propuesto añade un precepto según el cual la cooperación con las autoridades judiciales extranjeras sólo podrá denegarse cuando no exista norma jurídica que ampare la solicitud formulada y se determine la inexistencia de reciprocidad.

En este punto es necesario tener en cuenta que en la cooperación judicial en dicha materia se tratarán, con alta probabilidad, datos personales (de los posibles sospechosos, imputados, o testigos, etc.), por lo que las actuaciones de cooperación citadas han de cohonestarse con la legislación en materia de protección de datos personales. Más en concreto, toda cooperación con autoridades judiciales de países no pertenecientes a la Unión Europea habrá de tener en cuenta que la cooperación con dichas autoridades judiciales supondrá, normalmente, una transferencia de datos personales a terceros países, para lo cual la LO 7/2021, en su capítulo V (art. 43 y ss.) establece que:

1. *Al objeto de garantizar el nivel de protección de las personas físicas previsto en esta Ley Orgánica, **cualquier transferencia** de datos personales realizada **por las autoridades competentes españolas** a un Estado que no sea miembro de la Unión Europea o a una organización internacional, incluidas las transferencias ulteriores a otro Estado que no pertenezca a la Unión Europea o a otra organización internacional, deberá cumplir las siguientes condiciones:*

*a) Que la transferencia sea necesaria para los fines establecidos en el artículo 1.*

*b) Que los datos personales sean transferidos a un responsable del tratamiento competente para los fines mencionados en el artículo 1.*

*c) Que, en caso de que los datos personales hayan sido transferidos a la autoridad competente española procedentes de otro Estado miembro de la Unión Europea, dicho Estado miembro autorice previamente la transferencia ulterior de conformidad con su Derecho nacional.*

*d) Que la **Comisión Europea haya adoptado una decisión de adecuación** de acuerdo con el artículo 44 o, a falta de dicha decisión, cuando **se hayan aportado o existan garantías apropiadas de conformidad con el artículo 45** o, a falta de ambas, cuando resulten de aplicación las **excepciones para situaciones específicas de acuerdo con el artículo 46**.*

*e) Cuando se trate de una transferencia ulterior a un Estado que no sea miembro de la Unión Europea u organización internacional, de datos transferidos inicialmente por una autoridad competente española, esta autorizará la transferencia ulterior, una vez considerados todos los factores pertinentes, entre estos, la gravedad de la infracción penal, la finalidad para la que se transfirieron inicialmente los datos personales y el nivel de protección existente en ese Estado u organización internacional a los que se transfieran ulteriormente los datos personales.*

Ello supone que en la cooperación con autoridades judiciales de Estados no miembros de la UE habrá de tenerse en cuenta no sólo la existencia de un principio de reciprocidad, sino que aun no siendo necesario el recurso a este principio porque exista un tratado o convenio internacional, etc. habrá de existir una decisión de adecuación de la Comisión Europea conforme al art. 44 LO 7/2021 estableciendo que un Estado que no sea miembro de la Unión Europea garantiza un nivel de protección adecuado en materia de protección de datos personales. En defecto de dicha decisión de adecuación, conforme establece el art. 45 LO 7/2021, podrán realizarse transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional cuando concorra alguna de las siguientes circunstancias: a) Se hayan aportado garantías apropiadas respecto a la protección de datos personales en un instrumento jurídicamente vinculante (por ejemplo, en un tratado o convenio) o, b) se haya evaluado, por parte del responsable del tratamiento (la autoridad judicial etc.), todas las circunstancias que concurren en la transferencia de datos personales y se haya concluido que existen garantías apropiadas respecto a la protección de datos personales.

De ello resulta que dichos tratados, convenios, u otros instrumentos jurídicamente vinculantes habrán de establecer garantías apropiadas para transferir datos personales a dichas autoridades judiciales de terceros Estados en defecto de una decisión de adecuación de la Comisión Europea conforme al art. 44 LO 7/2021.

Si bien, conforme al art. 2.2, in fine LO 7/2021, dado que cuando los tratamientos los llevan a cabo jueces y magistrados del orden penal o fiscalías en asuntos penales “las autoridades de protección de datos a las que se refiere el capítulo VI no serán competentes para controlar estas operaciones de tratamiento”, no sería aplicable lo dispuesto en el art. 45.2 LO 7/2021, sí que en cualquier caso, deberían documentarse dichos tratamientos conforme al art.

45.3 LO 7/2021 cuando las transferencias se basen en lo dispuesto en el párrafo 1.b) del art. 45 LO 7/2021.

Por último, el art. 46 establece excepciones para la transferencia de datos a autoridades judiciales en situaciones específicas cuando no hay decisión de adecuación o garantías apropiadas conforme al art. 45 LO 7/2021. Entre ellas, singularmente, el art. 46.1, letras d) y sobre todo e), señalan como tales cuando es necesario para el ejercicio, en un caso individual, de acciones legales o para la defensa frente a ellas en relación con los fines incluidos en el artículo 1, de la LO 7/2021. En cualquier caso, el art. 45.2 especifica que los datos personales no se transferirán, si la autoridad competente de la transferencia determina que los derechos y libertades fundamentales del interesado prevalecen sobre el interés público en la transferencia, establecido en las letras d) y e) citadas. Por lo demás, y dado que la ley las califica como “excepciones”, dichas transferencias habrán de documentarse (fecha y hora de la transferencia, la información sobre la autoridad competente destinataria, la justificación de la transferencia y los datos personales transferidos), art. 46.3 LO 7/2021.

En definitiva, y como luego mencionaremos igualmente, al referirnos al contenido del artículo Cuarto del anteproyecto a la ley reguladora de los equipos conjuntos de investigación, la transferencia de datos personales en el ámbito de la cooperación judicial requiere que los acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial a terceros países se adapten a la normativa surgida de la LO 7/2021. Así, la Disposición Adicional segunda de la LO 7/2021 dice:

*Los acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial que impliquen la transferencia de datos personales a Estados que no sean miembros de la Unión Europea u organizaciones internacionales y que hubieran sido celebrados por España antes del 6 de mayo de 2016, cumpliendo lo dispuesto en el Derecho de la Unión Europea aplicable antes de dicha fecha, seguirán en vigor hasta que sean objeto de modificación, enmienda o terminación.*

## II

El artículo Segundo del Anteproyecto modifica la Ley de Enjuiciamiento Criminal (LECr) para establecer, según indica la Exposición de Motivos, una regulación mucho más completa del denominado Agente encubierto, hoy día regulado en el art. 282 bis LECr. Dicho precepto hace referencia igualmente al denominado “agente encubierto informático” (investigador bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de

comunicación), regulado también en dicho precepto y en los arts. 588 septies a) y siguientes de la LECR.

La Exposición de Motivos expone que se amplía la utilización de la medida de investigación del agente encubierto al delito de homicidio y sus formas agravadas. Igualmente reconoce que en cuanto intromisión extraordinaria en la intimidad de las personas afectadas, solo podrá entenderse justificada la utilización de este medio especial de investigación si la organización o grupo investigado presenta unos ciertos rasgos característicos, que centra, en definitiva, en la gravedad de los delitos investigados, o cuando sean menos graves, se den algunas de las circunstancias de los arts. 570 bis.2 y 570 ter.2 del Código Penal, es decir, deberá presentar una especial complejidad o peligrosidad que justifique el grado de injerencia que la utilización de esta diligencia implica, o bien existan actuaciones de grupos criminales terroristas o el delito de homicidio y sus formas agravadas. Se reconoce que la propia medida, en sí misma, supone una cierta intromisión en la intimidad, y que por ello no precisa una nueva autorización judicial para, por ejemplo, la entrada en domicilio del agente encubierto con el consentimiento -obviamente viciado- del investigado, pero que otras actuaciones -como por ejemplo una vigilancia acústica- sí la necesitarán.

Desde la perspectiva de la protección de datos personales, mediante el establecimiento de un agente encubierto, o de un agente informático encubierto, se realizan tratamientos de datos personales. El derecho a la protección de datos personales no es un derecho ilimitado, sino que puede ser limitado para proteger otros derechos fundamentales y bienes jurídicos constitucionalmente protegidos (STC 292/2000, FJ 11). Precisamente la LO 7/2021 establece los requisitos para la licitud de los tratamientos de datos personales a los fines del art. 1, que son, la prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

Así, el art. 11 LO 7/2021 requiere que *“cualquier ley que regule tratamientos de datos personales para los fines incluidos dentro del ámbito de aplicación de esta Ley Orgánica deberá indicar, al menos, los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento”*. Los objetivos y las finalidades de los tratamientos en el anteproyecto parece que quedan claros, pero no ocurre lo mismo con los datos personales que vayan a ser tratados en los tratamientos amparados por la regulación legal. Podrá ser relativamente complejo determinar qué datos personales va a ser objeto de estos tratamientos, pero así lo establece la ley para la licitud de dichos tratamientos en dicho art. 11. Este comentario sería aplicable a la totalidad del anteproyecto de ley.

No existe, por otra parte, en la Memoria de Análisis Normativo (MAIN) del anteproyecto, una referencia a la realización por el prelegislador de una

Evaluación de Impacto relativa a la Protección de Datos (EIPD). El art. 35 LO 7/2021 establece que *cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, suponga por su naturaleza, alcance, contexto o fines, un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.*

Parece razonable pensar que una actuación mediante un agente encubierto, físico o informático, supone un alto riesgo para el derecho fundamental a la protección de datos personales de los investigados, por más que pueda estar ciertamente justificada la intervención en dicho derecho constitucionales por la prevalencia en el caso concreto de otros derechos o intereses constitucionalmente legítimos. Dicha Evaluación de Impacto en materia de protección de datos (EIPD), conforme al art. 35.2 LO 7/2021, incluirá, *como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos peligros, así como las medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar su conformidad con la LO 7/2021.* La relación de datos personales que se prevé sean objeto del tratamiento habrá de resultar de dicha EIPD.

Esta AEPD ha venido insistiendo en la conveniencia, incluso en algunos casos, en la necesidad, de que cuando los tratamientos de datos personales vengan impuestos por la ley, se realice una EIPD cuando el legislador introduzca en el ordenamiento jurídico regulaciones que tengan especial trascendencia en los tratamientos de datos de carácter personal, de modo que previamente a la promulgación de la norma que lo regula se proceda a un análisis de los riesgos que puedan derivarse de dichos tratamientos, incluyendo en la MAIN un estudio sistematizado del impacto que en el derecho fundamental a la protección de datos personales de los interesados han de tener los distintos tratamientos de datos que prevea la ley (véase Informes 77/2020 o 97/2020, por ejemplo).

A este respecto, es preciso mencionar que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) establece expresamente (art. 3.1) que cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, 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, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o, en su ámbito competencial, por las autoridades autonómicas de



protección de datos, sin perjuicio de los requisitos establecidos en el mencionado real decreto. Añade expresamente (art. 3.2) que, 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 RGPD y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos (EIPD). En el Informe 072/2022 esta AEPD expuso, lo que ahora se reitera para el presente caso, regido por la LO 7/2021, que:

*[...] esta Agencia viene recomendando repetidamente en sus informes que el prelegislador, en aquellos casos, como el presente, en que los tratamientos tienen como base jurídica el art. 6.1.c) o e) del RGPD (esto es, tratamientos cuya base es una obligación legal o una misión de interés público o en ejercicio de poderes públicos), y venga establecida por el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento y tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, como es el caso de las operaciones de tratamiento derivadas de la LO 11/2021 o del presente reglamento de desarrollo, haga uso de la posibilidad que establece el art. 35.10 RGPD de modo **que sea el propio órgano proponente de la disposición general, en el curso del procedimiento de creación de la disposición de la norma (ley, real decreto, etc.) quien realice una evaluación de impacto relativa a la protección de datos (EIPD) como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica.** Dicha EIPD habrá de incorporarse, como permite -casi debería decirse que lo impone, pero en cualquier caso no lo prohíbe- el art. 2.1, letra g), del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo (MAIN). Este precepto es, además, suficientemente expresivo de la voluntad del legislador de incluir en la MAIN, dentro del concepto “Otros impactos”, el análisis del “impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma” (como es el caso de la base de datos referida en el art. 20 del proyectado reglamento).*

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

*Dicha EIPD no parece haberse llevado a cabo por el órgano proponente de la disposición general, o cuando menos, no se ha aportado a esta AEPD. Su realización permitiría que los responsables o encargados del tratamiento, una vez promulgada la norma, no tendrían la obligación de realizar dicha evaluación de impacto de datos personales (EIPD) prescrita en el art. 35 RGPD (y que el Real Decreto del ENS ha considerado asimismo obligatoria) precisamente por haberse llevado ya a cabo en el seno del proceso de gestación de la norma de carácter general.*

*Esta Agencia recuerda, asimismo, que el reiterado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) -que deroga al Real Decreto 3/2010, de 8 de enero, citado en la DA 4ª de la LO 11/2021- establece que la política de seguridad del sistema de información -esto es, la base de datos- deberá examinar y tener en cuenta “los riesgos que se derivan del tratamiento de los datos personales” (art. 12.1.f)), así como que en caso de que los sistemas de información traten datos personales (como es el caso), en todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto en caso de resultar agravadas respecto de las previstas en el citado real decreto (art. 3.3). Esto último, por otra parte, ya recogido en el apartado 11 de la DA 4ª de la LO 11/2021.*

*En definitiva, esta AEPD recomienda que se lleven a cabo, y se incorporen a la MAIN el análisis de riesgos (art. 24 RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD), lo que permitirá, a la vista de ello, al propio prelegislador, determinar no sólo las medidas de seguridad necesarias en los sistemas de información, sino las garantías específicas que se requieran para afrontar los riesgos derivados del tratamiento de los datos (ver art. 35.7.d) RGPD). Al no haber una EIPD no se conocen cuáles son esos riesgos que derivan del tratamiento generalizado y mecanizado, masivo, de datos personales que establece la norma, por lo que a esta Agencia no se le han ofrecido ni los riesgos ni en consecuencia las posibles medidas y garantías que paliarían esos riesgos.*

En el art. 282 quater, apartado 1, se sugiere que el contenido de la solicitud de la Policía Judicial de la medida del agente encubierto incorpore también, ya que no se hace mención en este apartado del precepto, cuáles son la información o informaciones que se pretenden obtener con la medida que se solicita del juez o del Ministerio Fiscal. En el apartado 3 de dicho art. 282 quater, en su letra d), el juez o el Ministerio Fiscal podrá valorar la pertinencia de la relevancia de dicha información o informaciones que se pretenden obtener a los efectos de la investigación, o ampliarla en su caso a otras, según



su razonado criterio. Esa concreción de la información solicitada contribuiría a centrar desde el principio la información que se pretende obtener, restringiendo así la afectación a los derechos de los interesados investigados, sin perjuicio, claro está, de la decisión judicial acerca de la extensión de la investigación.

El art. 282 sexies propuesto regula “el desarrollo de la investigación”, y, con una regulación más extensa que la del actual art. 282 bis, regula la necesidad de autorizaciones judiciales para la afectación de derechos fundamentales. A tal propósito, en su apartado 1, dicho art. 282 sexies se refiere a que la autorización judicial “ampara las actuaciones que realice en el curso de la investigación, aunque haya de verse afectado el derecho a la intimidad de las personas investigadas”. Esta Agencia considera que la actuación mediante Agente encubierto afecta directamente no sólo al derecho a la intimidad, sino que puede igualmente afectar al derecho fundamental a la protección de los datos personales del investigado o de las personas cuyos datos personales se recaban en dicha investigación (véase STC 115/2013, de 9 de mayo). Cabe recordar que el Tribunal Constitucional tiene declarado que el derecho a la protección de datos personales, aun cuando íntimamente ligado al derecho a la intimidad, es un derecho distinto e independiente, por cuanto tiene un objeto más amplio, y diferente. Así, la ya citada STC 292/2000, FJ 6º, expuso:

*De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.*

En definitiva, y para evitar que pueda considerarse que la autorización judicial no ampara la afectación directa al dicho derecho fundamental del investigado, se sugiere que el propuesto art. 282 sexies, en su apartado 1, contemple en su redacción, junto a la afectación al derecho a la intimidad, que la autorización judicial o fiscal de la intervención podrá afectar igualmente el derecho a la protección de datos personales de las personas investigadas:

*1. La autorización judicial o fiscal de la intervención del agente encubierto ampara las actuaciones que realice en el curso de la investigación, aunque haya de verse afectado el derecho a la intimidad o **el derecho a la protección de datos personales** de las personas investigadas*

En el art. 282 nonies se establece una posibilidad de utilización de las informaciones obtenidas mediante agente encubierto en otra investigación o procedimiento penal. Esta AEPD considera correcta dicha regulación, en cuanto se refiera a datos personales, pues la LO 7/2021 (art. 6.3) reconoce la posibilidad de que los datos personales cuyos tratamientos están regulados por dicha norma puedan ser tratados, por el mismo u otro responsable del tratamiento, para los fines del art. 1 de la ley (esto es, para 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) cuando se den cumulativamente las circunstancias de las letras a) y b) de dicho apartado. Dado que se prevé el tratamiento en el anteproyecto para una “investigación o procedimiento penal”, se cumpliría la circunstancia de la letra a), y al preverse que pueda resultar “necesaria para el esclarecimiento de un delito respecto del cual podría haberse acordado esta diligencia”, se considera que se cumpliría el requisito de la letra b). A ello se añade que la ley añade una cautela adicional, cual es la necesidad de autorización del Juez de instrucción competente para conocer de la nueva investigación.

En los arts. 282 decies.3, 282 duodecies.1.d) y 282 quaterdecies, párrafo segundo, se menciona la posibilidad de que el agente encubierto informático, con autorización judicial, intercambie archivos ilícitos por razón de su contenido.

La doctrina ha puesto de manifiesto que, en muchas ocasiones, el acceso de los agentes de la ley a las redes de delincuentes que utilizan lo que se denomina precisamente “canales cerrados de comunicación” requiere de estos que remitan archivos de contenido ilícito, los cuales, según los casos o el delito investigado, pueden contener material pornográfico que en muchas ocasiones recoge a menores de edad. Una posibilidad para la remisión o intercambio de dichos archivos sería recurrir a archivos que la policía se ha incautado en operaciones anteriores. Ahora bien, ello supone una afectación/intrusión muy relevante en el derecho a los datos personales (y su intimidad/propia imagen etc.) de dichos menores. Algún autor ha mencionado igualmente la posibilidad de utilizar vídeos con tecnología “deepfake” de menores que no existen en la realidad. Esta última posibilidad es, obviamente, ciertamente preferible a la primera, por cuanto no se vería envuelta ninguna

persona física realmente existente. No obstante, y en los supuestos en que ello no sea posible, ya por razones técnicas, de la propia investigación etc., el anteproyecto de ley, al igual que el actual art. 282 bis.6, requiere autorización judicial, pero no añade más. Hay consenso en la doctrina en que dicha autorización judicial ha de ser específica, distinta de la propia autorización judicial para el agente encubierto informático, aunque pueda estar incluida en esta, y basarse en los principios de idoneidad, necesidad y proporcionalidad. Ahora bien, lo que quiere resaltar esta AEPD es que esa decisión de poder intercambiar archivos ilícitos en que intervengan personas (mucho más aún menores de edad) ha de ser específicamente meditada por el Juez. Como puso de manifiesto el Informe del Consejo Fiscal al Anteproyecto de Ley de Reforma de la LECr. (pág. 450):

*La resolución judicial habilitante ha de tomar en consideración que la incorporación a la red de archivos de contenido ilícito puede determinar la puesta en riesgo de otros bienes jurídicos necesitados de protección, así como el riesgo de provocación delictiva que debe ser adecuadamente conjurado. Por ello, es necesario que en la misma se concrete la clase de archivo que se pretende introducir o intercambiar y el destino que se le da, valorando igualmente la posible pérdida de control de su recorrido en la red y, en su caso, la posibilidad o no de su posterior recuperación.*

Igualmente, dicho Informe del Consejo Fiscal (pág. 451) recogió que:

*Otra cuestión que debe ser puesta de relieve es la que se refiere a la identificación de los archivos ilícitos introducidos por el agente. Al respecto parece conveniente que el Anteproyecto, de forma expresa, exija que antes de la ejecución de esta medida se proceda a la adecuada identificación de los archivos que se introduzcan en la red. En realidad, esta es una condición ineludible, no solo para que pueda hacerse el seguimiento del archivo ilícito, sino también para que el juez pueda valorar, de acuerdo con criterios de proporcionalidad, la oportunidad o no de la medida*

En definitiva, se sugiere que el art. 282 duodecies, apartado 1, letra d), (o en un precepto o inciso específico) al referirse a la autorización por el juez de la medida de intercambiar o enviar archivos ilícitos, incluya alguna referencia expresa a que el juez habrá de autorizar expresamente no sólo la medida, sino identificar los archivos que se vayan a intercambiar, y en su resolución se valore la idoneidad, necesidad y proporcionalidad de dicha medida en relación con archivos ilícitos concretos que contengan imágenes de personas físicas, y con mayor intensidad si cabe si son menores.

El art. 588 septies c) recoge la nueva duración de la medida de registro remoto de equipos informáticos, medida que, como es obvio, afecta al derecho

a la protección de datos personales, por cuanto implica tener conocimiento de todos aquellos datos que puedan ser revelados sin el consentimiento de su titular por estar almacenados en el equipo terminal registrado en remoto.

Pues bien, el actual art. 588 septies c) establece una duración “máxima” de la medida de un mes, prorrogable por iguales períodos hasta un máximo de tres meses, mientras que el Anteproyecto sometido a informe establece una duración “inicial” (no “máxima”) de tres meses, prorrogables hasta un máximo de dieciocho. A este respecto es necesario mencionar que la MAIN no contiene explicación o razonamiento alguno a este aumento de la duración de la medida, o al cambio de “máxima” por “inicial”, y que el Anteproyecto de LECr. mantuvo el tenor de la redacción actual del vigente art. 588 septies c) LECr. (véase Informe Consejo Fiscal al Anteproyecto de LECr. pág. 383). En consecuencia, y habida cuenta del principio general de minimización de datos que se contiene en el art. 6.1, letra c) de la LO 7/2021, a falta de explicación, dicho tratamiento por dicho período podría considerarse excesivo.

### III

El artículo Tercero del anteproyecto modifica la ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea. Como su nombre indica, se refiere a resoluciones “penales”, incluidas dentro de la regulación de la ley (art. 1), y dentro de ellas se comprenden los instrumentos de reconocimiento mutuo del art. 2.2. Entre ellas, en la letra h), se incluye “[l]a resolución por la que se imponen sanciones pecuniarias”, reguladas en el título IX de la ley, arts. 173 y siguientes.

Pues bien, el anteproyecto modifica los artículos 173.1, 174.1 y 176.2, con el denominador común de suprimir la necesidad de que se trate de una sanción pecuniaria calificada como “penal”. En el texto anterior (es decir, el actualmente vigente), el art. 173.1 define “sanción pecuniaria” incluyendo las sanciones en concepto de multa aunque fueren impuestas como consecuencia de una infracción administrativa, pero con la particularidad de que dicha sanción debía de ser recurrible ante un órgano jurisdiccional “penal” para estar incluida en el ámbito de aplicación de la ley. El art. 174.2 establecía como autoridad competente para transmitir una resolución por la que se exija el pago de una sanción pecuniaria al órgano jurisdiccional “penal” competente para su ejecución en España, y el art. 176.2, al regular la transmisión de una resolución por la que se exija el pago de una sanción pecuniaria la confiaba a la autoridad judicial penal española.

La modificación propuesta suprime el adjetivo “penal” en todos estos casos, de manera que la definición de sanción pecuniaria englobaría toda sanción dineraria (por multa de tráfico, por ejemplo) meramente administrativa

sin relación alguna con ningún órgano jurisdiccional penal, puesto que todas las actuaciones administrativas son, en derecho español, recurribles ante un tribunal de justicia (art. 106 CE).

Como explicación para dicho cambio, la Memoria Abreviada de Análisis de Impacto Normativo (MAIN) expone tan sólo lo siguiente:

*Por lo que hace a la reforma de la Ley 23/2014, las modificaciones introducidas atañen a una regulación y distinción más precisa entre las causas imperativas y potestativas de denegación al reconocimiento y ejecución de determinados instrumentos de reconocimiento mutuo, la introducción de ajustes en los títulos que regulan el reconocimiento y ejecución de resoluciones de embargo y decomiso tras la aprobación del Reglamento (UE) 2018/1805, del parlamento europeo y del consejo de 14 de noviembre de 2018, sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso (a fin de evitar contradicciones entre la normativa nacional y el Reglamento, directamente aplicable), **así como mínimos ajustes en otros títulos, como el del reconocimiento mutuo de las resoluciones que imponen sanciones pecuniarias***

De manera igualmente concisa, la fundamentación que se contiene en la Exposición de Motivos al respecto dice:

*Por otra parte, se lleva a cabo a través de esta Ley la modificación de algunos aspectos de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea con el objetivo de depurar las **inconsistencias detectadas con el tenor literal de algunas de las decisiones marco de las que trae causa**, así, con en particular, armonizar la normativa nacional con lo dispuesto en el Reglamento (UE) 2018/2015, del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso.*

No se da por tanto explicación alguna acerca de por qué esos “mínimos ajustes” en la regulación de esos títulos, ni la razón de dichos cambios, o cuáles son esas “inconsistencias” detectadas con el tenor literal de algunas de las decisiones marco de las que trae causa, de suerte que resoluciones meramente administrativas, sancionatorias, pasen a estar consideradas, a efectos de la ley, como resoluciones “penales” (pues es precisamente esto lo que la ley ha de trasponer de la Decisión Marco citada); si ello es exigido por alguna sentencia del TJUE posterior a la ley que requiera dicha modificación, o por otras causa. De hecho, la ley 23/2014 menciona en su exposición de motivos la Decisión Marco 2005/214/JAI, de 24 de febrero de 2005, relativa a la aplicación del principio de reconocimiento mutuo de sanciones pecuniarias, que permite al Estado requirente acudir a la autoridad judicial del Estado en que la persona obligada al pago de una sanción pecuniaria derivada de la comisión de una infracción penal (“o administrativa en determinados casos”). Pero esos



“determinados casos” se establecen en el art. 1 de dicha Decisión Marco, según el cual, en todos los casos, la definición de “resolución” implica un carácter “penal”, normalmente acompañada de la revisión por un juez “penal”, cuestión esta que no estaría presente en la modificación presentada. De hecho, la regulación propuesta sería incompleta, puesto que elimina en el art. 174.1 la expresión “penal” para referirse al juez competente para transmitir una resolución, pero no tiene en cuenta que las sanciones “administrativas” no requieren, necesariamente, de un juez que las ejecute, dado el principio de autotutela, ejecutividad, ejecutoriedad y ejecución forzosa a través de sus propios órganos de que goza la Administración.

Sin perjuicio de cuestiones sustantivas, acerca de si determinadas sanciones elevadas impuestas por infracciones administrativas pueden tener la consideración de sanciones penales a los efectos de una posible doble instancia (véase sentencia del TEDH Saquetti Iglesias contra España, de 30 de junio de 2020, STC 71/2022, de 13 de junio, o STS 1.120/2022, de 8 de septiembre de 2022, Rec. 8160/2022) o si ciertas infracciones administrativas y sanciones graves pueden tener la consideración de datos especialmente protegidos por la normativa de protección de datos personales (véase por ejemplo STJUE de 22 de junio de 2021, C-439/19, apartados 90 y 91), nada se indica acerca de las razones de dicho cambio para que *todas* las resoluciones administrativas que impliquen una sanción pecuniaria pasen a estar incluidas en una ley que regula el reconocimiento recíproco de resoluciones “penales”, en el sentido que dicha ley y la Decisión marco citada establece. (Obsérvese, por otra parte, que el Anexo XII de la ley no se modifica, por lo que el apartado g) del mismo refleja aún las circunstancias de la ley previamente a la modificación que se pretende con el anteproyecto informado).

Quedaría pues, por otra parte, por coordinar, lo que no se menciona en el anteproyecto (o su MAIN), cuál sería el mecanismo aplicable para la ejecución de una determinada sanción administrativa, pues -sin perjuicio de lo mencionado acerca de que una sanción puede ejecutarse directamente por la Administración- una resolución administrativa sancionadora podrían ejecutarse tanto conforme a los mecanismos de la ley 23/2014, de reconocimiento mutuo de resoluciones penales en la Unión Europea, como con arreglo a la Directiva 2010/24/UE, de 16 de marzo de 2010, sobre la asistencia mutua en materia de cobro de los créditos correspondientes a determinados impuestos, derechos y otras medidas (véase art. 2 de esta), cuya transposición en España se contiene en la actualidad en la LGT, RGR etc.

Lo anteriormente expuesto tiene por otra parte su reflejo en materia de protección de datos personales, ya que los tratamientos de datos personales en materia “penal” se regulan por la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de

sanciones penales, y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, relativa, precisamente, a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Así, en los tratamientos de datos personales relativos a un proceso o ejecución “penal”, el tratamiento deberá llevarse a cabo según esta LO 7/201 citada, mientras que no siendo tratamientos “penales” (por ejemplo, los tratamientos en los cuales lo que se dilucida es una sanción meramente administrativa (no “penal”), dichos tratamientos deberán llevarse a cabo cumpliendo el RGPD, que tiene un régimen diferente.

Así, esta AEPD ya ha expresado (ver Informe 17/2021) que

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

*En lo que se refiere a los fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública, esta Agencia ha señalado que los mismos **sólo pueden interpretarse en relación con las infracciones y sanciones penales**, de manera que dado que el objeto de la Directiva es regular las normas relativas a la protección de las personas físicas respecto de los tratamientos de sus datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de infracciones penales, “incluidas” la protección y la prevención frente a las amenazas contra seguridad pública, dicha referencia a la prevención frente a las amenazas contra la seguridad pública **sólo puede referirse a aquellas amenazas que constituyan delito**. Cualquier tratamiento en relación con la prevención de amenazas a la seguridad pública que puedan constituir infracciones administrativas se regulará conforme al **RGPD, que establece mayores derechos para los interesados**.*

En definitiva, el RGPD establece mayores derechos para los interesados, por lo que cualquier tratamiento de datos personales que no se refiera a prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la

prevención frente a las amenazas contra la seguridad pública, lo que sería aplicable a infracciones y sanciones “meramente administrativas” (por oposición a sanciones “penales”) habrán de regirse por el RGPD, y no por la LO 7/2021.

A raíz de lo anterior, cabe mencionar que la única referencia que hace la ley 23/2014 a los datos personales se contiene en su art. 193, en su redacción dada por la ley 3/2018, de 11 de junio, relativo a la utilización en España de los datos personales obtenidos en la ejecución de la orden europea de investigación en otro Estado miembro. El anteproyecto sometido a informe no contiene ninguna modificación de la ley destinada al cumplimiento por esta de los requisitos que para los tratamientos de datos “penales” se recogen en la LO 7/2021, como por ejemplo el art. 11 de la LO 7/2021, que requiere que *[c]ualquier ley que regule tratamientos de datos personales para los fines incluidos dentro del ámbito de aplicación de esta Ley Orgánica [y esta ley/anteproyecto estaría aquí incluida] deberá indicar, al menos, los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento.*

Igualmente, y dado que el anteproyecto recoge igualmente tratamientos de datos “no penales”, como serían los tratamientos de datos para la ejecución etc., de sanciones meramente administrativas, habrían de regularse dichos tratamientos conforme al RGPD, como reconoce por otra parte expresamente el art. 6.2 LO 7/2021.

#### IV

El artículo Cuarto del anteproyecto establece una nueva ley reguladora de los equipos conjuntos de investigación, que sustituye a la Ley 11/2003, de 21 de mayo, reguladora de los equipos conjuntos de investigación penal en el ámbito de la Unión Europea. Esa nueva ley, introducida a su vez en un artículo del anteproyecto de ley, regula de manera unificada en el mismo texto los equipos conjuntos de investigación tanto con países de la UE como con terceros países, si bien se requiere autorización del Ministerio de Justicia en este último caso.

Se presenta aquí una situación similar a la descrita en el epígrafe I de este Informe, en el sentido de que en los equipos conjuntos de investigación se tratarán, con alta probabilidad, datos personales (de los posibles sospechosos, imputados, o testigos, etc.), por lo que las actuaciones de cooperación citadas han de cohonestarse con la legislación en materia de protección de datos personales. Así, a este respecto cabe reiterar que, como ya se ha expuesto en los epígrafes anteriores de este Informe, no hay en la MAIN mención ninguna a una evaluación de impacto de protección de datos (EIPD) que haga referencia a cuáles son los datos personales que previsiblemente se tratarán en los

tratamientos de datos que se produzcan conforme a esta ley, ni de los riesgos para los derechos de los interesados que se puedan derivar de dichos tratamientos, ni en consecuencia de las garantías que se establecen expresamente en la ley para evitar dichos riesgos. Ello supone, por añadidura, que la ley no ha indicado lo que resulta del art. 11.2 de la LO 7/2021: [c]ualquier ley que regule tratamientos de datos personales para los fines incluidos dentro del ámbito de aplicación de esta Ley Orgánica deberá indicar, al menos, los objetivos del tratamiento, los datos personales que vayan a ser objeto de este y las finalidades del tratamiento.

Toda cooperación de investigación mediante la creación de un equipo conjunto con autoridades de países no pertenecientes a la Unión Europea habrá de tener en cuenta que esta supondrá una transferencia de datos personales a terceros países.

En el art. 3 de la ley reguladora de los equipos conjuntos de investigación se necesita, para constituir equipos conjuntos de investigación con Estados terceros no miembros de la UE, “que exista una base legal habilitante para ello”, normalmente un convenio bilateral o multilateral que autorice y regule esta posibilidad. Conforme al art. 4 de la ley, los equipos conjuntos de investigación que constituyan las autoridades judiciales o policiales españolas se regirán por la normativa internacional habilitante para la constitución de este, por dicha Ley y por lo que se disponga en el acuerdo constitutivo, modificativo o de adhesión al equipo, cuyo contenido no podrá contravenir aquellas disposiciones.

Ello supone por tanto que en la cooperación con autoridades judiciales de Estados no miembros de la UE habrán de cumplirse igualmente las normas de protección de datos personales que habilitan para transferir datos a terceros Estados, y así habrá de existir una decisión de adecuación de la Comisión Europea conforme al art. 44 LO 7/2021. En defecto de dicha decisión de adecuación, conforme al art. 45 LO 7/2021, podrán realizarse transferencias de datos personales a un Estado que no sea miembro de la Unión Europea cuando concorra alguna de las siguientes circunstancias: a) Se hayan aportado garantías apropiadas respecto a la protección de datos personales en un instrumento jurídicamente vinculante (por ejemplo, el tratado o convenio con dicho país que autorice la creación de equipos conjuntos de investigación) o, b) se haya evaluado, por parte del responsable del tratamiento (la autoridad judicial etc.), todas las circunstancias que concurren en la transferencia de datos personales y se haya concluido que existen garantías apropiadas respecto a la protección de datos personales, debiendo documentarse, como regla el art. 45.3 LO 7/2021 cuando las transferencias se basen en lo dispuesto en el párrafo 1.b) del art. 45 LO 7/2021. Por último, el art. 46 establece excepciones para la transferencia de datos a autoridades judiciales en situaciones específicas, que ya hemos mencionado en el epígrafe I anterior, y que serían igualmente aplicables.

En definitiva, la transferencia de datos personales en el ámbito de la cooperación judicial, lo que incluiría el establecimiento de equipos conjuntos, requiere que los acuerdos internacionales que los regulen se adapten a la normativa surgida de la LO 7/2021. Así, recordamos que la Disposición Adicional segunda de la LO 7/2021 dice:

*Los acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial que impliquen la transferencia de datos personales a Estados que no sean miembros de la Unión Europea u organizaciones internacionales y que hubieran sido celebrados por España antes del 6 de mayo de 2016, cumpliendo lo dispuesto en el Derecho de la Unión Europea aplicable antes de dicha fecha, seguirán en vigor hasta que sean objeto de modificación, enmienda o terminación.*

El último párrafo del art. 4 preceptúa que “[e]n todos los casos, la actuación del equipo conjunto de investigación se someterá a las disposiciones de que en materia de protección de información clasificada o de protección de datos personales sean de aplicación, y especialmente a lo dispuesto en la Ley Orgánica 7/2021,(...)”, a lo que está AEPD informe favorablemente, por cuanto recoge el principio general establecido en la LO 7/2021 (art. 2.1), ya que las autoridades judiciales y policiales, en sus actuaciones en materia penal son “autoridades competentes” a los efectos del art. 4 de dicha ley, y la LO 7/2021 regula en todo caso los tratamientos de datos que estas autoridades lleven a cabo. Ello supone, por otra parte, que estas autoridades deben regirse por estas normas “en todo caso”, incluso en aquellos supuestos en los que las autoridades competentes de un tercer Estado tengan una normativa propia de protección de datos que no establezca una garantías similares para los interesados que las reguladas en esta ley. Los Tratados de carácter bilateral o multilateral que prevean la constitución de equipos conjuntos de investigación a que se refiere el art. 8 de la ley habrán de tener en cuenta estas circunstancias.

Asimismo, se sugiere que dentro del contenido del acuerdo de constitución del equipo conjunto de investigación a que se refiere el art. 11 de la ley se incluya, expresamente, una referencia a la normativa que regirá los tratamientos de datos que haya de llevarse a cabo en el desarrollo del equipo conjunto de investigación. Podría hacerse referencia tanto en la letra f) o en la letra h) del apartado 1, al mencionar la legislación aplicable a la actuación del equipo conjunto de investigación o al referirse al régimen jurídico sobre la utilización, por los miembros del equipo conjunto de investigación, de las informaciones obtenidas en el curso de la investigación.



El art. 16 regula el intercambio y uso de información bien directamente en las reuniones de coordinación que se celebren o a través de cualquier medio que garantice la confidencialidad y certeza de su contenido y la autenticidad de su transmisión, lo que es, directamente, una transferencia internacional de datos personales (cuando se intercambien datos referentes a personas físicas), por lo que es de aplicación todo lo expuesto anteriormente.

El apartado 2 de dicho artículo 16 regula la utilización de la información obtenida en el marco de un equipo conjunto de investigación. Si bien los tres primeros epígrafes de dicho apartado 2 (letras a), b) y c) serían conformes al art. 6.2 de la LO 7/2021, por cuanto harían referencia a los fines previstos en el art. 1 LO 7/2021 (esto es, 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), no ocurre lo mismo con la letra d) según la cual la información obtenida en el marco de un equipo conjunto de investigación, podrá utilizarse “[p]ara otros fines, siempre y cuando se hayan hecho constar en el acuerdo de constitución y en su caso de autorización”. El art. 6.2 LO 7/2021 es específico: *Los datos personales recogidos por las autoridades competentes no serán tratados para otros fines distintos de los establecidos en el artículo 1, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión Europea o por la legislación española. Cuando los datos personales sean tratados para otros fines, se aplicará el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión Europea.* En consecuencia, los datos personales recogidos por las autoridades competentes no pueden ser tratados para fines distintos de los del art. 1 de la LO 7/2021 (que ya se recogen en las letras a) a c) del art. 16.2 de la ley proyectada de equipos conjuntos), sin que dichos “otros” fines (que no se saben cuáles pueden ser) puedan establecerse “en el acuerdo de constitución y en su caso de autorización”, que no tienen rango legal suficiente; esos tratamientos para otros fines han de estar “autorizados por el Derecho de la Unión Europea o por la legislación española”, art. 6.2 LO 7/2021, y por supuesto no pueden contradecir la LO 7/2021 (véase art. 4 último párrafo de la ley proyectada) para permitir legitimar unos tratamientos de datos para fines distintos a los previstos en la LO 7/2021. Aun en el caso de que así fuera, el art. 6.2 LO 7/2021 recoge que dichos tratamientos para otros fines se regirían por el RGPD, lo cual no se menciona en el anteproyecto. En consecuencia, se informa desfavorablemente a este apartado d).