



2023/2131

11.10.2023

**REGLAMENTO (UE) 2023/2131 DEL PARLAMENTO EUROPEO Y DEL CONSEJO**

**de 4 de octubre de 2023**

**por el que se modifican el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo y la Decisión 2005/671/JAI del Consejo en lo que respecta al intercambio de información digital en casos de terrorismo**

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 85,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

De conformidad con el procedimiento legislativo ordinario <sup>(1)</sup>,

Considerando lo siguiente:

- (1) El Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo <sup>(2)</sup> creó Eurojust y establece sus funciones y competencias.
- (2) En la Decisión 2005/671/JAI del Consejo <sup>(3)</sup> se afirma que, para luchar contra el terrorismo, es esencial que los servicios pertinentes dispongan de la información más completa y actualizada posible. Dicha Decisión exige a las autoridades competentes de los Estados miembros proporcionar a Eurojust información sobre la instrucción de procesos penales y las condenas penales por delitos de terrorismo que afecten o puedan afectar a dos o más Estados miembros.
- (3) Debido a incoherencias en la interpretación de la Decisión 2005/671/JAI, en ocasiones la información no se comparte en el momento oportuno, no se comparte en absoluto o no toda la información pertinente se comparte. Eurojust necesita recibir información suficiente para detectar los vínculos entre investigaciones transfronterizas.
- (4) La asistencia a las autoridades competentes de los Estados miembros para garantizar la mejor coordinación posible de las investigaciones y actuaciones judiciales o del Ministerio Fiscal previas al juicio (en lo sucesivo, «investigaciones e instrucción en el proceso penal»), lo que incluye la detección de vínculos entre ellas, es una importante función de Eurojust en virtud del Reglamento (UE) 2018/1727. Dicho Reglamento permite que Eurojust adopte un enfoque más proactivo y ofrezca mejores servicios a los Estados miembros, por ejemplo, sugiriendo el inicio de investigaciones y detectando necesidades de coordinación, casos que pudieran vulnerar el principio *ne bis in idem* y lagunas durante la fase de instrucción del proceso penal.
- (5) En septiembre de 2019, sobre la base de la Decisión 2005/671/JAI, Eurojust creó el Registro Judicial Antiterrorista europeo con el objetivo específico de detectar posibles vínculos entre procedimientos judiciales contra sospechosos de delitos de terrorismo y las posibles necesidades de coordinación derivadas de esos vínculos.
- (6) El Registro Judicial Antiterrorista europeo se creó después de la adopción del Reglamento (UE) 2018/1727, por lo que no está correctamente integrado en la infraestructura técnica de Eurojust ni se le menciona en dicho Reglamento. Por lo tanto, es necesario subsanar dicha situación.
- (7) Para luchar contra el terrorismo de forma efectiva, es fundamental que las autoridades nacionales competentes y los organismos de la Unión intercambien entre ellos de manera eficaz información para la investigación o instrucción en el proceso penal de delitos de terrorismo. Es imprescindible contar con la información más completa y actualizada posible.

<sup>(1)</sup> Posición del Parlamento Europeo de 12 de julio de 2023 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 18 de septiembre de 2023.

<sup>(2)</sup> Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por [el] que se sustituye y deroga la Decisión 2002/187/JAI del Consejo (DO L 295 de 21.11.2018, p. 138).

<sup>(3)</sup> Decisión 2005/671/JAI del Consejo, de 20 de septiembre de 2005, relativa al intercambio de información y a la cooperación sobre delitos de terrorismo (DO L 253 de 29.9.2005, p. 22).

- (8) Las organizaciones terroristas participan cada vez más en otras formas de delitos graves y a menudo forman parte de redes organizadas. Se trata de una participación en delitos graves como la trata de seres humanos, el tráfico de drogas, los delitos económicos y el blanqueo de capitales. Es necesario cotejar la información sobre procedimientos judiciales contra tales delitos graves.
- (9) Con el fin de que Eurojust pueda detectar vínculos entre procedimientos judiciales transfronterizos contra sospechosos de delitos de terrorismo, así como vínculos entre procedimientos judiciales contra sospechosos de delitos de terrorismo e información tratada en Eurojust en relación con otros casos de delitos graves, es esencial que Eurojust reciba de las autoridades nacionales competentes lo antes posible, con arreglo a las disposiciones pertinentes del presente Reglamento, la información necesaria para que pueda detectar dichos vínculos mediante el cotejo de datos.
- (10) Para proporcionar datos a Eurojust, las autoridades nacionales competentes necesitan saber exactamente qué tipo de información deben transmitir, en qué fase del proceso penal nacional y en qué supuestos. Las autoridades nacionales competentes deben transmitir información a Eurojust de modo estructurado, organizado, sistemático y semiautomatizado. Un modo semiautomatizado es aquel en el que el modo utilizado para transmitir información está en parte automatizado y en parte controlado por personas. Se espera que dicho modo de transmisión aumente significativamente la calidad y la pertinencia de la información que recibe Eurojust.
- (11) La puesta en común, el almacenamiento y el cotejo de datos van a aumentar significativamente la cantidad de datos tratados por Eurojust. Estos elementos deben tenerse en cuenta a la hora de determinar, dentro de los procedimientos y marcos existentes, los recursos financieros, humanos y técnicos que precisa Eurojust.
- (12) La Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo (\*), según ha sido transpuesta al Derecho nacional, es el punto de referencia para que las autoridades nacionales competentes definan los delitos de terrorismo.
- (13) El intercambio de datos fiables de identificación es crucial para que Eurojust pueda detectar vínculos entre las investigaciones en materia de terrorismo y los procedimientos judiciales contra sospechosos de delitos de terrorismo. También es crucial que Eurojust tenga y conserve un conjunto de datos que garanticen la identificación fiable de las personas objeto de tales investigaciones o procedimientos. Por tanto, el uso de datos biométricos es importante si se tiene en cuenta la incertidumbre que rodea a los datos alfanuméricos —especialmente en el caso de los nacionales de terceros países—, el hecho de que, a veces, los sospechosos utilizan identidades falsas o dobles y que los datos biométricos son a menudo el único vínculo con los sospechosos en la fase de investigación. Por consiguiente, cuando, en virtud del Derecho procesal penal nacional o el Derecho nacional sobre derechos procesales en los procesos penales, las autoridades nacionales competentes almacenen y recojan datos biométricos y estén autorizadas a transmitirlos, deben poder intercambiar dichos datos con Eurojust cuando estén disponibles. Habida cuenta del carácter sensible de los datos biométricos y del efecto del tratamiento de tales datos en el respeto de la vida privada y familiar y en la protección de datos de carácter personal, consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, dichos datos deben transmitirse de manera que se respeten estrictamente los principios de necesidad, proporcionalidad y limitación de la finalidad, y únicamente con el fin de identificar a las personas que sean objeto de procesos penales relacionados con delitos de terrorismo.
- (14) Dado que la información sobre los vínculos existentes con otros procedimientos judiciales es más útil en una fase temprana de la investigación, es necesario que las autoridades nacionales competentes proporcionen información a Eurojust tan pronto como se remita el asunto a la autoridad judicial con arreglo a lo dispuesto en el Derecho nacional. Debe considerarse que un caso se ha remitido a una autoridad judicial cuando, por ejemplo, se le informe de una investigación en curso o cuando esta apruebe u ordene alguna medida de investigación o decida iniciar la instrucción en el proceso penal, en función del Derecho nacional aplicable. Si una autoridad nacional competente ya tiene conocimiento de la existencia de vínculos entre un proceso penal en su Estado miembro y un proceso penal en otro Estado miembro, debe informar de ello a Eurojust.

(\*) Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo (DO L 88 de 31.3.2017, p. 6).

- (15) Teniendo en cuenta que, en las tradiciones y los sistemas jurídicos de algunos Estados miembros, las autoridades judiciales no supervisan las investigaciones y solo participan en fases posteriores del proceso, el presente Reglamento no debe impedir que las autoridades nacionales competentes proporcionen información sobre investigaciones de terrorismo a sus miembros nacionales en una fase más temprana, de conformidad con su Derecho nacional.
- (16) Las autoridades nacionales competentes deben mantener actualizada la información que hayan proporcionado, con el fin de garantizar así la exactitud de los datos del Registro Judicial Antiterrorista europeo, detectar los vínculos o comprobar la identidad de un sospechoso lo antes posible en la investigación y garantizar que se respeten los plazos. Dichas actualizaciones deben incluir nueva información relativa a la persona investigada, resoluciones judiciales tales como la de prisión provisional, de inicio del juicio, de absolución y resoluciones de archivo o sobreseimiento definitivos, y solicitudes de cooperación judicial o vínculos detectados con otras jurisdicciones.
- (17) Las autoridades nacionales competentes no deben estar obligadas a compartir con Eurojust información sobre delitos de terrorismo en la fase procesal más temprana, cuando ello comprometa investigaciones en curso o la seguridad de una persona o cuando sea contrario a intereses esenciales de la seguridad del Estado miembro afectado. Tales excepciones a la obligación de compartir información solo deben aplicarse en circunstancias excepcionales y según el caso. Al considerar una posible excepción a tal obligación, las autoridades nacionales competentes deben tener debidamente en cuenta el hecho de que Eurojust trata la información proporcionada por dichas autoridades de conformidad con el Derecho de la Unión en materia de protección de datos y la confidencialidad de los procedimientos judiciales.
- (18) A efectos del intercambio de datos sensibles entre las autoridades nacionales competentes y Eurojust, así como de su tratamiento, y con objeto de proteger dichos datos contra la divulgación no autorizada y los ciberataques, deben utilizarse canales de comunicación seguros, como un sistema informático descentralizado o la conexión de telecomunicaciones segura a la que se refiere la Decisión 2008/976/JAI del Consejo <sup>(5)</sup>. Esta utilización debe entenderse sin perjuicio de futuros avances tecnológicos.
- (19) A fin de intercambiar datos de forma segura y proteger la integridad de la comunicación y el intercambio de datos, el sistema de gestión de casos debe estar conectado a canales de comunicación seguros y cumplir normas estrictas en materia de ciberseguridad. Dichos canales de comunicación seguros también pueden utilizarse para conectar el sistema de gestión de casos con otros sistemas de información de la Unión en la medida en que los actos jurídicos por los que se establecen dichos sistemas permitan el acceso de Eurojust.
- (20) El sistema informático descentralizado debe permitir el intercambio seguro de datos entre las autoridades nacionales competentes y Eurojust, sin participación de ninguna institución, órgano u organismo de la Unión en lo referente al contenido de dichos intercambios. El sistema informático descentralizado debe estar compuesto por sistemas informáticos dorsales (*back-end*) de los Estados miembros y Eurojust que estén interconectados por puntos de acceso interoperables. Los puntos de acceso del sistema informático descentralizado deben basarse en e-CODEX.
- (21) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento en lo que respecta al establecimiento y la utilización del sistema informático descentralizado para los supuestos objeto del presente Reglamento, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo <sup>(6)</sup>.
- (22) La transmisión de datos no estructurados hace necesaria la intervención manual, crea una carga administrativa adicional y reduce la calidad de los resultados del cotejo de información. Por consiguiente, las autoridades nacionales competentes deben transmitir los datos de manera estructurada, cumpliendo al mismo tiempo los requisitos mínimos de interoperabilidad definidos en el Marco Europeo de Interoperabilidad a que se refiere la Comunicación de la Comisión de 23 de marzo de 2017 titulada «Marco Europeo de Interoperabilidad – Estrategia de Aplicación». Por otra parte, la transmisión de datos debe automatizarse en la medida de lo posible para reducir la carga administrativa de las autoridades nacionales competentes y garantizar que los datos necesarios se proporcionen periódicamente y con celeridad.

<sup>(5)</sup> Decisión 2008/976/JAI del Consejo, de 16 de diciembre de 2008, sobre la Red Judicial Europea (DO L 348 de 24.12.2008, p. 130).

<sup>(6)</sup> Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

- (23) Para que Eurojust pueda tratar los datos personales sensibles de forma segura se necesita un sistema de gestión de casos modernizado. El nuevo sistema debe integrar y permitir las funcionalidades del Registro Judicial Antiterrorista europeo y mejorar la capacidad de Eurojust para detectar vínculos, al mismo tiempo que se aprovechan al máximo, como norma, los mecanismos nacionales y de la Unión existentes para comparar datos biométricos.
- (24) Es importante mantener el control y la responsabilidad de los miembros nacionales en relación con los datos que reciben de las autoridades nacionales competentes. Por defecto, no deben compartirse datos personales operativos con otro Estado miembro. Los datos personales operativos solo deben compartirse en la medida en que las autoridades nacionales competentes autoricen el intercambio de datos. Deben introducirse códigos de tratamiento con el fin de digitalizar y acelerar el seguimiento de los posibles vínculos, garantizando al mismo tiempo el pleno control de los datos.
- (25) El terrorismo y la delincuencia grave y organizada actuales son fenómenos muy dinámicos y globalizados que a menudo afectan a dos o más Estados miembros. Aunque el terrorismo ya tenía un fuerte componente transnacional, el uso y la disponibilidad de la comunicación electrónica han permitido un incremento significativo de la colaboración transnacional entre delincuentes terroristas. El carácter transnacional de un delito de terrorismo puede no conocerse cuando una autoridad judicial conoce del caso, pero puede revelarse durante el cotejo de datos por parte de Eurojust. Por lo tanto, la investigación o la persecución de los delitos terroristas requieren coordinación y cooperación entre las autoridades encargadas de ello o perseguirlos según criterios comunes, tal como se establece en el artículo 85 del Tratado de Funcionamiento de la Unión Europea (TFUE). La información sobre casos de terrorismo debe intercambiarse con Eurojust de manera oportuna, a menos que las circunstancias específicas del caso indiquen claramente que tiene un carácter puramente nacional.
- (26) Las investigaciones e instrucciones en procesos penales de casos de terrorismo se ven a menudo obstaculizadas por la falta de intercambio de información entre las autoridades nacionales de investigación y de instrucción o fiscales. Para poder cotejar nuevas investigaciones terroristas con investigaciones anteriores y detectar posibles vínculos, es necesario garantizar que el período de conservación de los datos sobre cualquier investigación anterior y sobre condenas sea adecuado para las actividades operativas. Por lo tanto, es necesario ampliar los plazos para el almacenamiento de datos en el Registro Judicial Antiterrorista europeo.
- (27) La posibilidad de cotejar nuevas investigaciones terroristas con investigaciones anteriores podría permitir detectar posibles vínculos e implicar la necesidad de cooperación. Este cotejo podría revelar que una persona sospechosa o imputada en un caso en trámite en un Estado miembro ha sido sospechosa o imputada en un caso concluido en otro Estado miembro. También podría detectar vínculos entre investigaciones o instrucciones en procesos penales en curso que de otro modo hubieran podido pasar desapercibidos. Esto sucede incluso cuando las investigaciones anteriores han concluido con una absolución o con una resolución de archivo o sobreseimiento definitivos. Es necesario pues, cuando proceda, almacenar los datos sobre cualquier investigación anterior, no solo sobre las condenas.
- (28) Es necesario garantizar que los datos de las investigaciones que hayan concluido con una absolución o con una resolución de archivo o sobreseimiento definitivos se traten únicamente a efectos de instrucción de los casos. Tales datos solo deben poder utilizarse a los efectos de detectar vínculos con investigaciones e instrucciones en procesos penales en curso y de apoyarlas. Salvo que la autoridad nacional competente decida lo contrario, teniendo en cuenta cada caso particular, Eurojust debe poder seguir tratando dichos datos operativos. Cuando, tras ganar firmeza la resolución de absolución o de archivo o sobreseimiento, la autoridad nacional competente decida que no es necesario el tratamiento de los datos de las personas absueltas o no acusadas, en particular, debido a las características específicas del caso o a los fundamentos de la absolución o del archivo o sobreseimiento, dichos datos deben suprimirse.
- (29) Eurojust ha celebrado doce acuerdos de cooperación con terceros países que permiten la transferencia de datos personales operativos a Eurojust y la asignación de destino en Eurojust de fiscales de enlace de terceros países. Además, el Acuerdo de Comercio y Cooperación entre la Unión Europea y la Comunidad Europea de la Energía Atómica, por una parte, y el Reino Unido de Gran Bretaña e Irlanda del Norte, por otra <sup>(7)</sup> permite destinar a un fiscal de enlace. En marzo de 2021, el Consejo otorgó a la Comisión un mandato para negociar acuerdos de cooperación entre Eurojust y otros trece terceros Estados, a saber, Argelia, Argentina, Armenia, Bosnia y Herzegovina, Brasil, Colombia, Egipto, Israel, Jordania, Líbano, Marruecos, Túnez y Turquía.

(7) DO L 149 de 30.4.2021, p. 10.

- (30) Si bien el Reglamento (UE) 2018/1727 proporciona una base jurídica para la cooperación y el intercambio de datos con terceros países, no incluye ninguna norma sobre los aspectos formales y técnicos de la cooperación con fiscales de enlace de terceros países destinados en Eurojust, en particular, en lo que se refiere a su acceso al sistema de gestión de casos. En aras de la seguridad jurídica, el Reglamento (UE) 2018/1727 debe proporcionar una base jurídica explícita para la cooperación entre Eurojust y los fiscales de enlace de terceros países y su acceso al sistema de gestión de casos. Eurojust debe aplicar salvaguardias y medidas de seguridad adecuadas para la protección de los datos y de los derechos fundamentales a través de la configuración técnica actualizada y de rigurosas normas internas.
- (31) Al tratar datos personales operativos de conformidad con el presente Reglamento, Eurojust debe garantizar un elevado nivel de protección de datos. Para el tratamiento de datos personales operativos, Eurojust debe atenerse al artículo 3 y al capítulo IX del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo <sup>(8)</sup>, así como a las normas específicas sobre el tratamiento de los datos personales operativos establecidas en el Reglamento (UE) 2018/1727, en su versión modificada por el Reglamento (UE) 2022/838 del Parlamento Europeo y del Consejo <sup>(9)</sup> y por el presente Reglamento. Dichas disposiciones se aplican al tratamiento de todos los datos personales operativos tratados por Eurojust. En particular, se aplican a todos los datos personales operativos tratados en el sistema de gestión de casos, ya sean tratados por miembros nacionales, corresponsales nacionales, fiscales de enlace u otras personas autorizadas de conformidad con el Reglamento (UE) 2018/1727.
- (32) Las decisiones sobre si Eurojust debe apoyar la coordinación y la cooperación entre las autoridades de investigación y de instrucción o fiscales, y en su caso de qué manera, deben corresponder exclusivamente a las autoridades competentes de los Estados miembros de que se trate, atendiendo al Derecho nacional aplicable, de la Unión o internacional, en particular, los convenios u otros acuerdos internacionales sobre asistencia judicial en materia penal.
- (33) En aras de la seguridad jurídica, conviene aclarar la relación entre el intercambio de información entre las autoridades nacionales competentes en materia de terrorismo y Eurojust en el marco de la Decisión 2005/671/JAI y del Reglamento (UE) 2018/1727. Por consiguiente, las disposiciones correspondientes deben suprimirse de la Decisión 2005/671/JAI y deben añadirse al Reglamento (UE) 2018/1727.
- (34) Aunque algunas autoridades nacionales competentes ya disponen de la conexión de telecomunicaciones segura a la que se refiere el artículo 9 de la Decisión 2008/976/JAI, muchas otras todavía no disponen de dicha conexión o de canales de comunicación seguros. A fin de garantizar que los Estados miembros dispongan de tiempo suficiente para proporcionar la referida conexión a las autoridades nacionales competentes, debe concederse un período transitorio para su implantación.
- (35) De conformidad con los artículos 1 y 2 y el artículo 4 *bis*, apartado 1, del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea (TUE) y al TFUE, y sin perjuicio del artículo 4 de dicho Protocolo, Irlanda no participa en la adopción del presente Reglamento y no queda vinculada por él ni sujeta a su aplicación.
- (36) De conformidad con los artículos 1 y 2 del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al TUE y el TFUE, Dinamarca no participa en la adopción del presente Reglamento y no queda vinculada por él ni sujeta a su aplicación.
- (37) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, del Reglamento (UE) 2018/1725, emitió su dictamen el 26 de enero de 2022.

<sup>(8)</sup> Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

<sup>(9)</sup> Reglamento (UE) 2022/838 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, por el que se modifica el Reglamento (UE) 2018/1727 en lo que respecta a la preservación, análisis y almacenamiento en Eurojust de pruebas relativas al genocidio, los crímenes contra la humanidad, los crímenes de guerra y las infracciones penales conexas (DO L 148 de 31.5.2022, p. 1).

HAN ADOPTADO EL PRESENTE REGLAMENTO:

### Artículo 1

#### Modificación del Reglamento (UE) 2018/1727

El Reglamento (UE) 2018/1727 se modifica como sigue:

- 1) En el artículo 3, el apartado 5 se sustituye por el texto siguiente:

«5. Eurojust podrá prestar también asistencia en las investigaciones y la instrucción en procesos penales que únicamente afecten a un Estado miembro y un tercer país, o a un Estado miembro y una organización internacional, siempre que se haya celebrado con dicho país u organización internacional algún convenio de cooperación o algún acuerdo por el que se entable una cooperación en virtud del artículo 52, o siempre que en un caso concreto exista un interés esencial en prestar dicha asistencia.

La decisión de si los Estados miembros prestan asistencia judicial a un tercer país o a una organización internacional, y de qué manera lo hagan, corresponderá únicamente a la autoridad competente del Estado miembro afectado, atendiendo al Derecho nacional aplicable, de la Unión o internacional.».

- 2) El artículo 20 se modifica como sigue:

- a) se inserta el apartado siguiente:

«2 bis. Cada Estado miembro designará a una autoridad nacional competente como corresponsal nacional de Eurojust en materia de terrorismo. Dicho corresponsal nacional en materia de terrorismo será una autoridad judicial u otra autoridad competente. Cuando así lo exija el ordenamiento jurídico nacional, el Estado miembro podrá designar a más de una autoridad nacional competente como corresponsal nacional de Eurojust en materia de terrorismo. El corresponsal nacional en materia de terrorismo tendrá acceso a toda la información pertinente de conformidad con el artículo 21 bis, apartado 1. Será competente para recabar dicha información y transmitirla a Eurojust, de conformidad con el Derecho nacional y de la Unión, en particular, el Derecho procesal penal nacional y las normas aplicables en materia de protección de datos.»;

- b) el apartado 8 se sustituye por el texto siguiente:

«8. Para alcanzar los objetivos a los que hace referencia el apartado 7 del presente artículo, las personas contempladas en el apartado 3, letras a), b) y c), del presente artículo, deberán estar conectadas al sistema de gestión de casos con arreglo a lo dispuesto en el presente artículo y en los artículos 23, 24, 25 y 34. Los costes de conexión al sistema de gestión de casos correrán a cargo del presupuesto general de la Unión.».

- 3) El artículo 21 se modifica como sigue:

- a) el apartado 9 se sustituye por el texto siguiente:

«9. El presente artículo no afectará a otras obligaciones relativas a la transmisión de información a Eurojust.»;

- b) el apartado 10 se sustituye por el texto siguiente:

«10. Las autoridades nacionales competentes no estarán obligadas a proporcionar información con arreglo a lo dispuesto en el presente artículo, si dicha información ya hubiera sido transmitida a Eurojust de conformidad con otras disposiciones del presente Reglamento.».

- 4) Se inserta el artículo siguiente:

«Artículo 21 bis

#### Intercambio de información sobre casos de terrorismo

1. Por lo que se refiere a los delitos de terrorismo, las autoridades nacionales competentes informarán a sus miembros nacionales de cualquier investigación penal en curso o finalizada supervisada por autoridades judiciales, tan pronto como el caso se remita a las autoridades judiciales de conformidad con lo dispuesto en el Derecho nacional, en particular, el Derecho procesal penal nacional, de cualquier instrucción en un proceso penal y cualquier

proceso judicial que esté en curso o haya finalizado y de cualquier resolución judicial sobre delitos de terrorismo. Dicha obligación se aplicará a todas las investigaciones penales relacionadas con delitos de terrorismo, con independencia de que exista un vínculo conocido con otro Estado miembro o con un tercer país, a menos que la investigación penal, debido a sus circunstancias específicas, afecte claramente a un único Estado miembro.

2. El apartado 1 no se aplicará cuando:

- a) el intercambio de información comprometa una investigación en curso o la seguridad de una persona, o
- b) el intercambio de información sea contrario a intereses de seguridad esenciales del Estado miembro de que se trate.

3. A efectos del presente artículo, se entenderá por “delitos de terrorismo” los delitos a que se refiere la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo (\*).

4. La información transmitida de conformidad con el apartado 1 incluirá los datos personales operativos y los datos no personales que figuran en el anexo III. Dicha información podrá incluir datos personales de conformidad con el anexo III, letra d), únicamente si tales datos personales están en poder de las autoridades nacionales competentes o pueden ser comunicados a estas con arreglo al Derecho nacional y si la transmisión de dichos datos es necesaria para identificar de manera fiable a un interesado a efectos de lo dispuesto en el artículo 27, apartado 5.

5. Sin perjuicio de lo dispuesto en el apartado 2, las autoridades nacionales competentes informarán a sus miembros nacionales de cualquier cambio en la información transmitida en virtud del apartado 1 sin demora indebida y, en la medida de lo posible, en un plazo máximo de diez días hábiles después del cambio.

6. La autoridad nacional competente no estará obligada a proporcionar dicha información si ya ha sido transmitida a Eurojust.

7. La autoridad nacional competente podrá solicitar en cualquier momento el apoyo de Eurojust en el marco de las medidas de seguimiento relacionadas con los vínculos detectados a partir de la información suministrada con arreglo al presente artículo.

(\*) Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo (DO L 88 de 31.3.2017, p. 6).».

5) Se insertan los artículos siguientes:

«Artículo 22 bis

### **Comunicación digital segura e intercambio de datos entre las autoridades nacionales competentes y Eurojust**

1. La comunicación entre las autoridades nacionales competentes y Eurojust en el marco del presente Reglamento se llevará a cabo a través del sistema informático descentralizado. El sistema de gestión de casos a que se refiere el artículo 23 estará conectado a una red de sistemas informáticos y puntos de acceso e-CODEX interoperables, que funcionan bajo la responsabilidad y la gestión individuales de cada Estado miembro y Eurojust, lo que hace posible un intercambio transfronterizo de información seguro y fiable (en lo sucesivo, “sistema informático descentralizado”).

2. Cuando el intercambio de información de conformidad con el apartado 1 no sea posible debido a la indisponibilidad del sistema informático descentralizado o debido a circunstancias excepcionales, se llevará a cabo por el medio alternativo más rápido y adecuado. Los Estados miembros y Eurojust velarán por que los medios de comunicación alternativos sean fiables y ofrezcan un grado equivalente de seguridad y protección de datos.

3. Las autoridades nacionales competentes transmitirán a Eurojust la información de los registros nacionales a la que se refieren los artículos 21 y 21 bis del presente Reglamento de modo semiautomatizado y estructurado. La Comisión determinará las modalidades de dicha transmisión, en consulta con Eurojust, en un acto de ejecución, de conformidad con el artículo 22 ter del presente Reglamento. En particular, dicho acto de ejecución determinará el formato de los datos transmitidos de conformidad con lo dispuesto en el anexo III, letra d), del presente Reglamento, así como las normas técnicas necesarias relativas a la transmisión de dichos datos, y establecerá las especificaciones de procesamiento digital tal como se definen en el artículo 3, punto 9, del Reglamento (UE) 2022/850 del Parlamento Europeo y del Consejo (\*).

4. La Comisión se encargará de la creación, el mantenimiento y el desarrollo de un programa informático de aplicación de referencia que los Estados miembros y Eurojust podrán decidir utilizar como sistema dorsal (*back-end*). Dicho programa informático de aplicación se basará en una configuración modular, lo que significa que el programa informático se empaqueta y se entrega separado de los componentes e-CODEX necesarios para conectarlo al sistema informático descentralizado. Dicha configuración permitirá a los Estados miembros reutilizar o mejorar sus infraestructuras nacionales existentes de comunicación judicial con fines de uso transfronterizo y hacer posible que Eurojust conecte su sistema de gestión de casos al sistema informático descentralizado.

5. La Comisión proporcionará, mantendrá y prestará apoyo al programa informático de aplicación de referencia gratuitamente. La creación, el mantenimiento y el desarrollo del programa informático de aplicación de referencia se financiarán con cargo al presupuesto general de la Unión.

6. Los Estados miembros y Eurojust sufragarán sus respectivos costes de establecimiento y funcionamiento de un punto de acceso e-CODEX autorizado tal como se define en el artículo 3, punto 3, del Reglamento (UE) 2022/850, y de establecimiento y adaptación de sus sistemas informáticos pertinentes para que sean interoperables con los puntos de acceso.

#### Artículo 22 ter

### Adopción de actos de ejecución por la Comisión

1. La Comisión adoptará los actos de ejecución necesarios para el establecimiento y la utilización del sistema informático descentralizado para la comunicación en el marco del presente Reglamento, en los que se establecerá lo siguiente:

- a) las especificaciones técnicas que determinen los modos de comunicación por medios electrónicos a los efectos del sistema informático descentralizado;
- b) las especificaciones técnicas de los protocolos de comunicación;
- c) los objetivos en materia de seguridad de la información y las medidas técnicas pertinentes que garanticen las normas mínimas de seguridad de la información y unas normas de alto nivel en materia de ciberseguridad para el tratamiento y la comunicación de información dentro del sistema informático descentralizado;
- d) los objetivos mínimos de disponibilidad y los posibles requisitos técnicos relacionados para los servicios prestados por el sistema informático descentralizado;
- e) la creación de un comité de dirección, que incluya representantes de los Estados miembros, para garantizar el funcionamiento y el mantenimiento del sistema informático descentralizado a fin de cumplir los objetivos del presente Reglamento.

2. Los actos de ejecución a que se refiere el apartado 1 del presente artículo se adoptarán a más tardar el 1 de noviembre de 2025 de conformidad con el procedimiento de examen a que se refiere el artículo 22 quater, apartado 2.

#### Artículo 22 quater

### Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo (\*\*).



2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

Cuando el comité no emita ningún dictamen, la Comisión no adoptará el proyecto de acto de ejecución y se aplicará el artículo 5, apartado 4, párrafo tercero, del Reglamento (UE) n.º 182/2011.

(\*) Reglamento (UE) 2022/850 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a un sistema informatizado para el intercambio electrónico transfronterizo de datos en el ámbito de la cooperación judicial en materia civil y penal (sistema e-CODEX), y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 150 de 1.6.2022, p. 1).

(\*\*) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).».

6) Los artículos 23, 24 y 25 se sustituyen por el texto siguiente:

«Artículo 23

#### **Sistema de gestión de casos**

1. Eurojust establecerá un sistema de gestión de casos para el tratamiento de los datos personales operativos mencionados en el anexo II, los datos enumerados en el anexo III y los datos no personales.

2. El sistema de gestión de casos tendrá por objeto:

- a) apoyar la gestión y la coordinación de las investigaciones e instrucciones en procesos penales en las que Eurojust presta asistencia;
- b) garantizar el acceso seguro y el intercambio de información sobre las investigaciones e instrucciones en procesos penales en curso;
- c) permitir el cotejo de la información y la detección de vínculos;
- d) permitir la extracción de datos con fines operativos y estadísticos;
- e) facilitar la supervisión para garantizar que el tratamiento de los datos personales operativos es lícito y cumple el presente Reglamento y las normas aplicables en materia de protección de datos.

3. El sistema de gestión de casos podrá conectarse a la red de telecomunicaciones segura mencionada en el artículo 9 de la Decisión 2008/976/JAI del Consejo (\*) y a otros canales de comunicación seguros, de conformidad con el Derecho de la Unión aplicable.

4. Cuando se haya concedido a Eurojust acceso a datos que figuren en otros sistemas de información de la Unión establecidos en virtud de otros actos jurídicos de la Unión o que provengan de dichos sistemas, Eurojust podrá utilizar el sistema de gestión de casos para acceder a los datos que figuran en esos sistemas o para conectarse a esos sistemas de información con el fin de obtener y tratar información, incluidos los datos personales, a condición de que sea necesario para el desempeño de sus funciones y se atenga a lo dispuesto en los actos jurídicos de la Unión que establecen tales sistemas de información.

5. Los apartados 3 y 4 no amplían los derechos de acceso a otros sistemas de información de la Unión concedidos a Eurojust en virtud de los actos jurídicos de la Unión que establecen dichos sistemas.

6. En el desempeño de sus funciones, los miembros nacionales podrán tratar datos personales de los casos concretos en los que estén trabajando, de conformidad con el presente Reglamento u otros instrumentos aplicables. Deberán permitir que el delegado de protección de datos tenga acceso a los datos personales tratados en el sistema de gestión de casos.

7. Para el tratamiento de los datos personales operativos, Eurojust no podrá crear ningún archivo de datos automatizado distinto del sistema de gestión de casos.

Los miembros nacionales podrán almacenar temporalmente datos personales y analizarlos para determinar si presentan interés para las funciones de Eurojust y pueden ser incluidos en el sistema de gestión de casos. Dichos datos podrán conservarse durante tres meses como máximo.

#### Artículo 24

##### **Gestión de la información en el sistema de gestión de casos**

1. El miembro nacional conservará la información que se le haya transmitido de conformidad con el presente Reglamento u otros instrumentos aplicables en el sistema de gestión de casos.

El miembro nacional será responsable de la gestión de los datos que haya tratado.

2. El miembro nacional decidirá, teniendo en cuenta cada caso particular, si mantiene la restricción de acceso a la información o si da acceso a esta, en su totalidad o en parte, a otros miembros nacionales, a los fiscales de enlace destinados en Eurojust, a personal autorizado de Eurojust o a cualquier otra persona que trabaje por cuenta de Eurojust que haya recibido la necesaria autorización del director administrativo.

3. El miembro nacional indicará, en consulta con las autoridades nacionales competentes, en términos generales o específicos, cualquier restricción al posterior manejo, acceso y transmisión de la información si se ha detectado uno de los vínculos mencionados en el artículo 23, apartado 2, letra c).

#### Artículo 25

##### **Acceso al sistema de gestión de casos en el ámbito nacional**

1. Las personas a las que se refiere el artículo 20, apartado 3, letras a), b) y c), no tendrán acceso más que a los datos siguientes:

- a) los datos controlados por el miembro nacional de su Estado miembro;
- b) los datos controlados por miembros nacionales de otros Estados miembros y a los cuales el miembro nacional de su Estado miembro haya obtenido acceso, a menos que el miembro nacional que controle los datos haya denegado tal acceso.

2. Los miembros nacionales, dentro de las limitaciones establecidas en el apartado 1 del presente artículo, decidirán sobre el alcance del acceso que se conceda en su Estado miembro a las personas a las que se refiere el artículo 20, apartado 3, letras a), b) y c).

3. Los corresponsales nacionales de Eurojust en asuntos de terrorismo a los que se refiere el artículo 20, apartado 3, letra c), serán los únicos que puedan acceder en el ámbito nacional a los datos suministrados de conformidad con lo dispuesto en el artículo 21 bis.

4. Cada Estado miembro podrá decidir, tras consultar a su miembro nacional, que las personas a las que se refiere el artículo 20, apartado 3, letras a), b) y c), puedan introducir en el sistema de gestión de casos, dentro de las limitaciones previstas en los apartados 1, 2 y 3 del presente artículo, información relativa a su Estado miembro. Esta contribución requerirá la validación del miembro nacional correspondiente. El Colegio fijará los detalles de aplicación práctica del presente apartado. Los Estados miembros notificarán a Eurojust y a la Comisión su decisión relativa a la aplicación del presente apartado. La Comisión informará de ello a los demás Estados miembros.

(\*) Decisión 2008/976/JAI del Consejo, de 16 de diciembre de 2008, sobre la Red Judicial Europea (DO L 348 de 24.12.2008, p. 130).».

7) El artículo 27 se modifica como sigue:

a) el apartado 4 se sustituye por el texto siguiente:

«4. Eurojust podrá tratar categorías especiales de datos personales operativos de conformidad con el artículo 76 del Reglamento (UE) 2018/1725. Cuando estos otros datos se refieran a testigos o víctimas en el sentido del apartado 2 del presente artículo, la decisión de tratarlos deberán tomarla de forma conjunta los miembros nacionales concernidos.»;

b) se añade el apartado siguiente:

«5. Cuando se transmitan datos personales operativos de conformidad con el artículo 21 *bis*, Eurojust podrá tratar los datos personales operativos enumerados en el anexo III de las siguientes personas:

a) las personas respecto de las que, de conformidad con el Derecho nacional del Estado miembro en cuestión, existan motivos fundados para creer que han cometido o están a punto de cometer un delito que recaiga dentro de las competencias de Eurojust;

b) las personas que hayan sido condenadas por tal delito.

Salvo que la autoridad nacional competente decida otra cosa en el caso concreto de que se trate, Eurojust podrá seguir tratando los datos personales operativos a que se refiere el párrafo primero, letra a), también después de que haya concluido el procedimiento con arreglo al Derecho nacional del Estado miembro de que se trate, incluso en caso de absolución o de resolución de archivo o sobreseimiento definitivos. Si el procedimiento no ha dado lugar a una condena, el tratamiento de datos personales operativos solo podrá efectuarse al objeto de detectar vínculos entre las investigaciones e instrucciones en procesos penales en curso, futuros o concluidos en el sentido de lo dispuesto en el artículo 23, apartado 2, letra c).».

8) El artículo 29 se modifica como sigue:

a) se inserta el apartado siguiente:

«1 *bis*. Eurojust no conservará los datos personales operativos transmitidos de conformidad con el artículo 21 *bis* después de aquella de las siguientes fechas que acontezca primero:

a) la fecha en que haya expirado el plazo de prescripción del delito en todos los Estados miembros afectados por la investigación o la instrucción en el proceso penal;

b) cinco años después de la fecha en que adquiera firmeza la resolución judicial del último de los Estados miembros afectados por la investigación o la instrucción en el proceso penal o dos años en caso de absolución o de resolución de archivo o sobreseimiento definitivos;

c) la fecha en que Eurojust sea informada de la resolución de la autoridad nacional competente con arreglo al artículo 27, apartado 5.»;

b) los apartados 2 y 3 se sustituyen por el texto siguiente:

«2. El cumplimiento de los plazos de conservación establecidos en los apartados 1 y 1 *bis* permanecerá bajo examen constante mediante un tratamiento automatizado apropiado realizado por Eurojust, especialmente, a partir del momento en que Eurojust deje de prestar apoyo.

La necesidad de conservar los datos también será objeto de examen cada tres años tras la introducción de los datos.

Si los datos personales operativos a que se refiere el artículo 27, apartado 4, se conservan durante un período superior a cinco años, se informará de ello al SEPD.

3. Antes de que expire alguno de los plazos de conservación establecidos en los apartados 1 y 1 *bis*, Eurojust examinará la necesidad de prolongar la conservación de los datos personales operativos, cuando y mientras ello sea necesario para el desempeño de sus funciones.

Podrá decidir seguir conservando a título excepcional dichos datos hasta el siguiente ejercicio de examen. Los motivos de la prolongación de la conservación deberán justificarse y registrarse. De no tomarse una decisión sobre la prolongación de la conservación de los datos personales operativos en el momento del examen, dichos datos se suprimirán automáticamente.».

9) Se inserta el artículo siguiente:

«Artículo 54 bis

#### **Fiscales de enlace de terceros países**

1. Un fiscal de enlace de un tercer país podrá ser destinado a Eurojust sobre la base de un acuerdo de cooperación que permita dicho destino y que se haya celebrado antes del 12 de diciembre de 2019 entre Eurojust y dicho tercer país o de un acuerdo internacional celebrado entre la Unión y el tercer país con arreglo al artículo 218 del TFUE que permita dicho destino de un fiscal de enlace.

2. Los derechos y obligaciones del fiscal de enlace se establecerán en el acuerdo de cooperación o en el acuerdo internacional a que se refiere el apartado 1, o en un acuerdo de trabajo celebrado de conformidad con el artículo 47, apartado 3.

3. Se concederá acceso a los fiscales de enlace destinados en Eurojust al sistema de gestión de casos para el intercambio seguro de datos. De conformidad con los artículos 45 y 46, Eurojust seguirá manteniendo responsabilidad por el tratamiento de datos personales por parte de los fiscales de enlace en el sistema de gestión de casos.

Las transferencias de datos personales operativos a los fiscales de enlace de terceros países a través del sistema de gestión de casos solo podrán realizarse con arreglo a las normas y condiciones establecidas en el presente Reglamento, en el acuerdo con el país correspondiente o en otros instrumentos jurídicos aplicables.

El artículo 24, apartado 1, párrafo segundo, y el artículo 24, apartado 2, se aplicarán *mutatis mutandis* a los fiscales de enlace.

El Colegio establecerá las condiciones detalladas de acceso.».

10) En el artículo 80, se añaden los apartados siguientes:

«9. Eurojust podrá seguir utilizando el sistema de gestión de casos compuesto por expedientes temporales de trabajo y un índice hasta el 1 de diciembre de 2025, si para entonces aún no se ha implantado el nuevo sistema de gestión de casos.

10. Las autoridades nacionales competentes y Eurojust podrán seguir utilizando otros canales de comunicación distintos de los mencionados en el artículo 22 bis, apartado 1, hasta el primer día del mes siguiente al período de dos años posterior a la fecha de entrada en vigor del acto de ejecución a que se refiere el artículo 22 ter del presente Reglamento, si para entonces los canales de comunicación a que se refiere el artículo 22 bis, apartado 1, aún no están disponibles para el intercambio directo entre ambos.

11. Las autoridades nacionales competentes podrán seguir proporcionando información de otra forma que no sea semiautomática de conformidad con el artículo 22 bis, apartado 3, hasta el primer día del mes siguiente al período de dos años posterior a la fecha de entrada en vigor del acto de ejecución a que se refiere el artículo 22 ter del presente Reglamento, si para entonces aún no se han implantado los requisitos técnicos.».

11) Se añade el anexo siguiente:

«ANEXO III

a) información para identificar a la persona sospechosa, acusada, condenada o absuelta:

Personas físicas:

— apellido(s),

— nombre,

- alias, en su caso,
- fecha de nacimiento,
- lugar de nacimiento (ciudad y país),
- nacionalidad(es),
- documento de identificación (tipo y número del documento),
- sexo,
- lugar de residencia.

Personas jurídicas:

- razón social,
- forma jurídica,
- lugar de la sede central.

Personas tanto físicas como jurídicas:

- número(s) de teléfono,
- correo(s) electrónico(s),
- datos de cuentas en bancos o en otras entidades financieras;

b) información sobre el delito de terrorismo:

- información sobre las personas jurídicas implicadas en la preparación o comisión de un delito de terrorismo,
- calificación jurídica del delito con arreglo al Derecho nacional,
- forma de delincuencia grave aplicable de la lista a que se refiere el anexo I,
- pertenencia a un grupo terrorista (si la hubiera),
- tipología de terrorismo (como, por ejemplo, yihadista, separatista, de izquierda o de derecha),
- breve exposición del caso;

c) información sobre el procedimiento nacional:

- estado del procedimiento,
- fiscalía competente,
- número del expediente,
- fecha de inicio del procedimiento judicial formal,
- vínculos con otros casos pertinentes;

d) información adicional para identificar a la persona sospechosa:

- datos dactiloscópicos recogidos de conformidad con el Derecho nacional durante el proceso penal,
- fotografías.».

*Artículo 2*

**Modificación de la Decisión 2005/671/JAI**

La Decisión 2005/671/JAI se modifica como sigue:

- 1) En el artículo 1, se suprime la letra c).
- 2) El artículo 2 se modifica como sigue:
  - a) se suprime el apartado 2;

b) el apartado 3 se sustituye por el texto siguiente:

«3. Cada Estado miembro adoptará las medidas necesarias para garantizar que al menos la información a que se refiere el apartado 4 relativa a las investigaciones penales por delitos de terrorismo que afecten o puedan afectar a dos o más Estados miembros, recabada por la autoridad competente, se transmita a Europol, de conformidad con el Derecho nacional y con el Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo (\*).

(\*) Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DO L 135 de 24.5.2016, p. 53).»;

c) se suprime el apartado 5.

### Artículo 3

#### Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en los Estados miembros de conformidad con los Tratados.

Hecho en Estrasburgo, el 4 de octubre de 2023.

*Por el Parlamento Europeo*

*La Presidenta*

R. METSOLA

*Por el Consejo*

*El Presidente*

J. M. ALBARES BUENO