

# LA COOPERACIÓN POLICIAL EN EL SENO DE EUROPOL: EL PRINCIPIO DE DISPONIBILIDAD Y LA CONFIDENCIALIDAD DE LA INFORMACIÓN<sup>1</sup>

Police cooperation in the Europol: The principle  
of availability and the confidentiality of the information

JUANA GOIZUETA VÉRTIZ

Universidad del País Vasco/Euskal Herriko Unibertsitatea  
juana.goizueta@ehu.eus

## *Cómo citar/Citation*

Goizueta Vértiz, J. (2017).

La cooperación policial en el seno de Europol: el principio de disponibilidad  
y la confidencialidad de la información.

*Revista Española de Derecho Constitucional*, 110, 75-103.

doi: <https://doi.org/10.18042/cepc/redc.110.03>

## **Resumen**

El tratamiento e intercambio de la información resulta clave para preservar una eficaz cooperación policial en la lucha y erradicación de la delincuencia transnacional y el terrorismo. Una cooperación policial que se articula a través de Europol y que persigue aumentar el grado de seguridad de los ciudadanos en el Espacio de Libertad, Seguridad y Justicia. Ahora bien, la mayor seguridad o el afán de incrementar la eficacia policial en la lucha contra el terrorismo y la delincuencia transfronteriza no debe suponer, en general, una menor protección de los derechos humanos y las libertades individuales y, en particular, no ha de mermar el derecho a la intimidad y a la protección de los datos personales. En este contexto, en el presente trabajo, se aborda

---

<sup>1</sup> El presente trabajo ha sido realizado en el marco del proyecto de investigación del MINECO ref. DER 2014-57116-P, dirigido por Aida Torres y Maribel González Pascual, y de la ayuda del Departamento de Educación, Universidades e Investigación del Gobierno Vasco al grupo de investigación consolidado dedicado al tema de los «Derechos Fundamentales y UE Europea» (GIC07/86-IT-448-07).

el tratamiento de la información desde la perspectiva de las autoridades competentes estatales lo que ha exigido el estudio del principio de la disponibilidad que se articula jurídicamente a través de la Decisión Marco 2006/960/ JAI y del principio de la confidencialidad regulado en la Decisión 2009/371 que es desarrollada por la Decisión 2009/968.

### ***Palabras clave***

Europol; cooperación policial; principio de disponibilidad; principio de confidencialidad; tratamiento de la información.

### ***Abstract***

The exchange and processing of information are a key to preserve an effective police cooperation in combating and eliminating of the transnational crime and terrorism. A police cooperation that is structured via Europol and seeks to increase the level of safety of citizens in the Area of Freedom, Security and Justice. However, the greater security or effort to increase the police effectiveness in combating terrorism and cross-border crime should not assume, in general, less protection of human rights and individual freedoms, and in particular, decreasing the right to privacy and protection of personal data. In this context, this work deals with processing of information since the perspective of the competent state authorities, which has required the study of the principle of availability, it is legally structured through the Framework Decision 2006/960/JHA, and principle of confidentiality regulated in the Decision 2009/371 and developed by the Decision 2009/968.

### ***Keywords***

Europol; police cooperation; principle of availability; principle of confidentiality; processing of information.

## SUMARIO

---

I. LA COOPERACIÓN POLICIAL Y EUROPOL. II. EUROPOL COMO AGENCIA EUROPEA DE POLICÍA: 1. El tratado de Lisboa y la nueva situación jurídica de Europol: Europol como agencia de la UE. 2. Organización y funcionamiento de Europol. 3. Función y competencias de Europol. III. EL TRATAMIENTO DE LA INFORMACIÓN COMO FORMA DE COOPERACIÓN: 1. El principio de disponibilidad de la información: 1.1. *El intercambio de información entre los servicios de seguridad españoles competentes y los servicios de seguridad competentes de otros Estados miembros.* 1.2. *El intercambio de información con Europol.* 2. La confidencialidad de la información. IV. CONSIDERACIONES FINALES. BIBLIOGRAFÍA.

---

### I. LA COOPERACIÓN POLICIAL Y EUROPOL

En el marco del denominado Espacio de Libertad, Seguridad y Justicia, se prevé, tal y como se desprende del art. 67.3 del Tratado de Funcionamiento de la Unión Europea (TFUE), la cooperación como fórmula para garantizar un nivel elevado de seguridad en la Unión Europea (UE). Y entre los diversos tipos de cooperación, se encuentra la de tipo policial<sup>2</sup>, que se materializa en el seno de Europol y que, junto con la de naturaleza judicial, se erige en un instrumento necesario para poder luchar y combatir de modo eficaz las diferentes modalidades de delincuencia transnacional y el terrorismo.

Son diversas las formas de cooperación policial interna<sup>3</sup> que se materializan en el seno de Europol en su relación con los Estados miembros, pudiendo encuadrarse nuestra pretensión dentro del contexto del tratamiento de la información por Europol o a través de Europol. Recordemos que la consecución de los objetivos de esta agencia europea de policía y, por ende, de los objetivos de la cooperación policial pasan por el tratamiento de la información entendida en los siguientes términos:

[...] cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales o no personales,

---

<sup>2</sup> Los fundamentos jurídicos de la cooperación policial se encuentran en los arts. 87, 88 y 89 TFUE.

<sup>3</sup> Téngase en cuenta la distinción entre *cooperación externa* y *cooperación interna*. La primera hace referencia a la que se articula con los Estados miembros de la UE, mientras que la denominada cooperación exterior se refiere a la que materializa Europol con organizaciones y países terceros a través de acuerdos de cooperación.

como la recogida, registro, organización, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, así como su bloqueo, eliminación o destrucción<sup>4</sup>.

De modo que bien podría sostenerse que el tratamiento de la información constituye una herramienta destinada a la consecución de una eficaz cooperación policial y que resulta clave en la prevención y lucha contra la criminalidad organizada.

En efecto, precisamente ese tratamiento de la información centrará nuestra atención en el presente trabajo en tanto en cuanto conforma la base de la cooperación policial. Un tratamiento que será abordado desde la óptica que afecta a las autoridades estatales competentes lo que exigirá analizar tanto el principio de la disponibilidad de la información como el llamado *principio de confidencialidad*. Para ello, tras este apartado I introductorio en el que realizamos una serie de apreciaciones de índole genérico sobre la cooperación policial, abordaremos el estudio de Europol partiendo de su nuevo *status quo* diseñado con el Tratado de Lisboa haciendo especial hincapié en aspectos relativos a su organización y funcionamiento, así como a su función y competencias (apartado II). Posteriormente, nos ocuparemos del tratamiento de la información efectuado por o a través de Europol desde la perspectiva estatal, lo que exigirá analizar su encaje con el principio de la disponibilidad y, asimismo, abordar el estudio de la confidencialidad de la información (apartado III). Y, para finalizar, la última parte del trabajo la dedicaremos a las consideraciones finales (apartado IV).

## II. EUROPOL COMO AGENCIA EUROPEA DE POLICIA

### 1. EL TRATADO DE LISBOA Y LA NUEVA SITUACIÓN JURÍDICA DE EUROPOL: EUROPOL COMO AGENCIA DE LA UE

El 26 de julio de 1995 se firma en Bruselas el convenio por el que se establece una oficina europea de policía denominado Convenio Europol<sup>5</sup>. Si bien,

<sup>4</sup> Así se define el «tratamiento de la información» en el art. 1 de la Decisión 2009/968/JAI del Consejo, de 30 de noviembre de 2009, por la que se adoptan las normas sobre confidencialidad de la información de Europol (en lo sucesivo, Decisión 2009/968) (DOUE L 332/17, de 17 de diciembre de 2009).

<sup>5</sup> DOUE C núm. 316, de 27 de noviembre de 1995, y BOE núm. 232, de 28 de septiembre de 1998.

Europol comienza su andadura en julio de 1999 tras la entrada en vigor del citado convenio el 1 de octubre de 1998 que será modificado en diversas ocasiones aumentando el ámbito de actuación competencial de la Agencia en diferentes campos de intervención<sup>6</sup>.

Y es a través de la Decisión del Consejo 2009/371/JAI, de 6 de abril de 2009 (en adelante, Decisión 2009/371<sup>7</sup>) cuando Europol se convierte en una agencia comunitaria financiada con cargo al presupuesto general de la UE<sup>8</sup>, con lo que se atiende al doble objetivo de simplificar y mejorar el marco jurídico de la Agencia y reforzar el control que sobre la misma ejerce el Parlamento Europeo. En este sentido, bien puede afirmarse que en 2009 se produce la modificación de su naturaleza jurídica, a saber, se le atribuye el estatuto de agencia o «ente de la Unión» según la literalidad de la propia decisión. Un estatuto jurídico que se mantiene actualmente con la aprobación del Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la UE 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 (en adelante, Reglamento Europol)<sup>9</sup>. Un reglamento en el que, siguiendo el art. 77, se diferencia entre fecha de entrada en vigor y fecha a partir de la cual será aplicable. La entrada en vigor se prevé tras una *vacatio legis* de veinte días desde su publicación en el *Diario Oficial de la Unión Europea* el 24 de mayo de 2016, lo que nos sitúa el 13 de junio de 2016, aunque se difiere la aplicación del Reglamento Europol hasta el 1 de mayo de 2017. De ello se deduce que la derogación de la Decisión 2009/371 y, por ende, su sustitución por el Reglamento Europol se retrasa hasta el 1 de mayo de 2017. Si bien es cierto que, el propio Reglamento Europol contempla una excepción a esa regla general de la aplicación a partir del 1 de mayo de 2017, estableciéndose un período de transitoriedad que abarca

---

<sup>6</sup> Primero, este convenio fue complementado por dos protocolos firmados el 24 de julio de 1996 y el 19 de junio de 1997 (publicados en el DO C núm. 299, de 9 de octubre de 1996, y en el DO C 221, de 19 de julio de 1997, respectivamente) y, posteriormente, fue modificado por otros tres protocolos firmados el 30 de noviembre de 2000 (DO C núm. 358, de 13 de diciembre de 2000), el 28 de noviembre de 2002 (DO C núm. 312, de 16 de diciembre de 2002) y el 27 de noviembre de 2003 (DO C núm. de 6 de enero de 2004).

<sup>7</sup> Sobre la Decisión 2009/371, resulta interesante De Moor (2010).

<sup>8</sup> Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol), DO L núm. 121, de 15 de mayo de 2009, pp. 37-66. En particular, véase el art. 42 de la reseñada decisión.

<sup>9</sup> DOUE L135/53, de 24 de mayo de 2016.

del 13 de junio del presente hasta el 1 de mayo de 2017 con relación a algunas cuestiones relativas al Consejo de Administración, a la figura del director ejecutivo y a la de los directores adjuntos. Así pues, y hasta el 1 de mayo de 2017, como regla general rige la Decisión 2009/371.

En efecto, Europol actualmente es una agencia de la UE que opera en el Espacio de Libertad, Seguridad y Justicia destinada a constituirse en el interlocutor principal en el ámbito de la actuación policial —tanto desde un punto de vista preventivo como represivo— en el seno de la UE. Europol es, en definitiva, la Oficina Europea de Policía, que conforma un elemento clave de cooperación internacional en aras de combatir la delincuencia organizada transfronteriza<sup>10</sup> y que simboliza el modelo europeo de inteligencia criminal (Del Moral Torres, 2010: 1). En suma, el Tratado de Lisboa sitúa a Europol en una nueva situación jurídica y la equipara, en cuanto a su naturaleza, a otros entes que operan en ámbitos cubiertos por el título VI TUE, tales como Eurojust o la Cepol. A día de hoy Europol, tal y como se establece en el art. 62 del Reglamento Europol, es una agencia de la UE a la que se le reconoce personalidad jurídica y que está llamada a ejercer un papel clave en lo que se refiere a mejorar el intercambio de inteligencia entre los Estados (Bosilca, 2013:17) en aras de la prevención y erradicación de las diversas modalidades de delincuencia grave a nivel internacional.

## 2. ORGANIZACIÓN Y FUNCIONAMIENTO DE EUROPOL

Por lo que respecta a la organización regulada en el capítulo VI de la Decisión 2009/371, cabe advertir que Europol la integran, principalmente, además del Consejo de Administración<sup>11</sup> y su director<sup>12</sup>, cientos de oficiales

<sup>10</sup> Resulta significativo el siguiente dato: se contabilizan anualmente en más de 12 000 los casos de delincuencia grave y terrorismo a los que Europol presta ayuda.

<sup>11</sup> Nótese que —atendiendo a la ya aludida transitoriedad de las disposiciones relativas al Consejo de Administración contenida en el art. 72 del Reglamento Europol— la duración del mandato de los miembros del Consejo de Administración finalizará el 1 de mayo de 2017 a quien se le encomienda la preparación de los instrumentos necesarios para la aplicación del Reglamento, en particular, de las medidas relacionadas con el tratamiento de la información. A lo que cabe añadir que es el 14 de diciembre de 2016 la fecha límite prevista para que los Estados miembros notifiquen a la Comisión los nombres de quienes han de integrar el nuevo Consejo de Administración que celebrará su primera reunión el 1 de mayo de 2017.

<sup>12</sup> Si bien su mandato es de cuatro años prorrogable una sola vez, atendiendo al art. 73 del Reglamento Europol, este mandato se prorrogará automáticamente hasta el 1 de mayo de 2018 en el caso de que el mismo expirara entre el 13 de junio de 2016 y el 1

pertenecientes a distintas agencias y órganos de seguridad de los Estados miembros, incluyendo servicios de fronteras, autoridades policiales, personal de aduanas y otras autoridades competentes en la materia<sup>13</sup>. Su sede radica en La Haya y cuenta con una unidad central en la que trabajan unos 130 funcionarios u oficiales de enlace adscritos a Europol que conectados a través de una red excepcional están distribuidos en las distintas unidades nacionales sitas en las capitales de los distintos Estados miembros. Estas unidades nacionales de cada Estado miembro deben garantizar una cooperación eficaz entre Europol y los Estados miembros y constituyen el punto de contacto entre la Agencia y las autoridades competentes de estos Estados.

La red de oficiales de enlace acoge a funcionarios de los Estados miembros de la UE en un entorno operativo seguro y cabe señalar que cada unidad nacional cuenta, al menos, con un funcionario de enlace en comisión de servicios en Europol<sup>14</sup>. Estos funcionarios de enlace conectan cada unidad nacional con Europol y presentan y protegen los intereses de la unidad en el seno de Europol. Las unidades nacionales ubicadas en cada uno de los Estados parte de la UE<sup>15</sup> son las encargadas de proporcionar la información a Europol, corregirla o cancelarla definitivamente y ejercer su actividad en estrecha coordinación con los funcionarios de enlace.

Con relación a su funcionamiento, debe evidenciarse siguiendo a Nunzi (2007) que Europol funciona con base en el criterio de la colaboración mutua y con la intervención de la unidad central de Europol, las unidades nacionales, los funcionarios nacionales de enlace y el sistema de información de Europol, al que se incorporan los datos y al que nos referiremos en el siguiente

---

de mayo de 2017. Y, también, con base en el reseñado art. 73 del Reglamento Europol, el director de la Agencia puede asumir durante el tiempo que le resta de mandato, las funciones de director ejecutivo con arreglo al art. 16 del Reglamento. Y solo cuando este no pueda o no quiera asumir tales funciones el Consejo de Administración designará un director ejecutivo interino para ejercerlas por un período máximo de dieciocho meses.

<sup>13</sup> En concreto, podemos decir que Europol cuenta con 698 personas en la sede principal.

<sup>14</sup> Aunque, no puede obviarse que, además la Agencia cuenta con oficiales de enlace de diez países y organizaciones no pertenecientes a la UE que colaboran amparados en acuerdos de cooperación. A todo ello habría que añadir los dos oficiales de enlace en Washington DC y el oficial de la sede de Interpol en Lyon.

<sup>15</sup> La sede de la Unidad Nacional de Europol (UNE) española radica en el Complejo Policial de Canillas en Madrid y constituye, junto con Interpol y la Oficina Sirene, la Unidad de Cooperación Policial Internacional dentro de la Comisaría General de Policía Judicial del Cuerpo Nacional de Policía.

apartado de este trabajo. En este sentido, cabe señalar que los funcionarios de enlace, por ejemplo, participan en todos los proyectos de análisis; asimismo, toman parte en las reuniones operativas, ejercen una labor de coordinación, por ejemplo, en las labores de vigilancia transnacional, o asesoran y ejercen de enlace con los expertos nacionales para la creación de equipos conjuntos de investigación.

Antes de pasar al examen de la función y competencias de Europol, únicamente debo apuntar que en su funcionamiento conforma una piedra angular el centro operativo permanente de coordinación y apoyo de Europol encargado de verificar la información que llega de diferentes fuentes y países y que permanece activo los siete días de la semana durante veinticuatro horas al día. Un centro operativo permanente que conforma el único punto para el intercambio de datos entre la Agencia, los Estados miembros y terceros, a saber, Estados no miembros de la UE situados geográficamente fuera de Europa.

### 3. FUNCIÓN Y COMPETENCIAS DE EUROPOL

Es el art. 88 TFUE el que prevé la función llamada a ejercer por Europol. Y en el marco de este paraguas, en concreto, la Decisión 2009/371 realiza en su art. 5 un listado del amplio abanico de funciones atribuidas a la Agencia que van desde la recogida, almacenamiento, tratamiento, análisis e intercambio de información de datos a la prestación de asistencia en diferentes ámbitos a los Estados miembros para responder a su objetivo pasando por la facilitación de apoyo analítico a los Estados miembros o la realización de investigaciones y actividades operativas en el marco de la participación en equipos conjuntos de investigación<sup>16</sup> y, en su caso, en colaboración con Eurojust<sup>17</sup>. Y

---

<sup>16</sup> Se empleó esta dinámica de equipos conjuntos de investigación (ECI), compuestos por autoridades policiales y judiciales por citar un ejemplo, en el caso de la denominada Operación Golf. En concreto, es el Servicio de Policía Metropolitana de Londres quien crea un ECI con las autoridades rumanas —en particular, se adscribieron dos funcionarios policiales rumanos a Londres— con el fin de llevar a cabo una investigación sobre el problema de las redes organizadas de trata de seres humanos compuestas por romaníes de origen rumano que se produce en Londres. Estamos ante el primer ECI que investigó este tipo de delitos en Europa logrando identificar a 181 menores que eran víctimas de trata de seres humanos. Sobre los ECI, véase Pérez Gil (2007: 65-79).

<sup>17</sup> Así se operó en el caso de una banda de *aluzinadores* de nacionalidad lituana que operaban en Austria, pero con conexión con Bélgica, Francia, Italia y Suecia. En este



es que no puede obviarse que la prevención y la lucha de las diferentes formas grave de criminalidad internacional exigen para ser eficaces de un planteamiento común (Bonn, 2007: 34)<sup>18</sup>.

Acerca de la asistencia operativa señalar que son los funcionarios policiales de los Estados miembros de la UE los beneficiarios de esta y que tal asistencia se presta bajo diversas modalidades, entre otras: asistencia a través de la oficina móvil integrada por analistas y expertos; apoyo *in situ* para prestar colaboración a operaciones policiales; o apoyo forense y técnico en diferentes ámbitos, tales como fraude de tarjetas de pago, falsificación del euro, fabricación de artículos falsificados, ciberdelincuencia o desmantelamiento de centros de producción, almacenamiento y eliminación de drogas ilegales.

Tras este breve recorrido, cabe avanzar que nos situamos, en efecto, ante un listado generoso de atribuciones en el que la información y los datos cobran una especial relevancia (Niemeier y Wiegand, 2010: 169-194).

Con relación a las competencias de la Agencia, entendidas estas como posibles ámbitos materiales de su actuación, el art. 4 de la Decisión del año 2009 diferencia los dos siguientes bloques:

- De una parte, se refiere a la delincuencia organizada, el terrorismo<sup>19</sup> y otras formas de delitos graves siempre que dos o más Estados se vean afectados lo que significa que el carácter transfronterizo constituye una pieza clave para la intervención de Europol. La referencia a

---

caso concreto, se organizó por Eurojust una reunión de coordinación a los efectos de planificar la intervención en Lituania. Y, asimismo, se actuó en coordinación con Eurojust en la denominada Operación Creieur.

<sup>18</sup> Como prueba de la necesidad del planteamiento común y la cooperación transfronteriza para lograr la eficacia en este contexto puede traerse a colación la Red Camden de Recuperación de Bienes (CARIN) de la que forman parte los Estados miembros de la UE y que responde al objetivo de facilitar la cooperación transfronteriza en materia de seguimiento, bloqueo, incautación y confiscación de activos provenientes de actividades delictivas.

<sup>19</sup> Téngase en cuenta que el 10 de agosto de 2010 entró en vigor el Acuerdo entre la UE y Estados Unidos relativo al tratamiento y la transferencia de datos de mensajería financiera de la UE a efectos del programa de seguimiento de la financiación del terrorismo (TFTP), por el que recae sobre Europol la responsabilidad de verificar si las solicitudes de transferencia de datos provenientes de Estados Unidos cumplen las cláusulas pactadas en el mencionado acuerdo. Asimismo, hay que constatar que, atendiendo a lo previsto en el Convenio, se ha creado en el seno de Europol una unidad específica de especialistas y analistas financieros en materia de lucha contra el terrorismo que cooperan activamente con las autoridades estadounidenses.

otras formas de delitos graves se concreta vía anexo en la propia Decisión 2009/371 en la que se mencionan, a título ejemplificativo, las siguientes: tráfico ilícito de estupefacientes<sup>20</sup>, actividades ilícitas de blanqueo de capitales<sup>21</sup>, delitos relacionados con materiales nucleares o sustancias radiactivas, tráfico de inmigrantes clandestinos<sup>22</sup>, etc.<sup>23</sup>. Y es que, si bien, en sus inicios, Europol centró sus

---

<sup>20</sup> La lucha contra los delitos relacionados con las drogas son una de las grandes prioridades de Europol desde su creación, de modo que Europol lleva prestando su ayuda al Grupo de Drogas Sintéticas de Cospol (Planificación Estratégica Operativa General de la Policía) desde 2005. Y también es de destacar en la lucha contra los delitos relacionados con las drogas, el Sistema Europol de Comparación de Laboratorios Ilegales (EILCS, por sus siglas en inglés) que contiene información fotográfica y técnica detallada sobre centros de producción, almacenamiento y eliminación de drogas sintéticas. Y el Sistema Europol de Drogas Sintéticas (ESDS, por sus siglas en inglés) que incluye información sobre *modus operandi* y decomisos importantes.

Nos interesa destacar que la ayuda operativa de Europol en esta área de actuación comprende la coordinación y puesta en marcha de investigaciones penales, la ayuda sobre el terreno a los servicios policiales de la UE en labores de desmantelamiento de instalaciones ilícitas dedicadas a producir drogas sintéticas, ayudando a la policía a la recogida de pruebas que se consideren necesarias, y la realización de investigaciones técnicas relativas a los equipos caseros e industriales aprehendidos en las unidades de producción y almacenamiento de estupefacientes. Y pasando al plano de la concreción, cabe señalar que las redes de delincuencia organizada relacionadas con la cocaína en Europol quedan incluidas en un proyecto específico que incorpora un fichero de análisis a lo que cabe añadir la existencia del Proyecto Cannabis de Europol que nace en marzo de 2010.

<sup>21</sup> En esta área delictiva la colaboración de Europol se centra en el análisis de operaciones sospechosas desde el punto de vista financiero.

<sup>22</sup> En este orden de cosas, Europol otorga ayuda analítica a los Estados miembros de la UE para combatir la facilitación de la inmigración ilegal, elabora informe de datos y facilita el intercambio de información. Este proyecto analítico se ha dividido en subproyectos. En concreto, en 2010 hubo siete subproyectos centrados en inmigración ilegal. También Europol ha participado desde agosto de 2010 en un equipo de investigación conjunta sobre matrimonios de conveniencia dentro de este proyecto analítico y en esta área de actuación hemos de encuadrar, para concluir, la operación Alcázar.

<sup>23</sup> Nótese que la Decisión 2009/371, en el anexo, incluye el mismo elenco de delitos graves que figura en la Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre los Estados miembros, DO L 190 de 18 de julio de 2002. Y en particular, se hace referencia a los siguientes: explotación sexual de menores; trata de seres

esfuerzos en el ámbito de la lucha contra la droga en la actualidad, es bastante generoso el ámbito de actuación en el que interviene, incluyéndose un tipo de delincuencia no estrictamente relacionada con la delincuencia organizada.

- Y, de otra parte, se mencionan como competencias de Europol, también, los delitos penales conexos: un tipo delictivo que el art. 4.3 concreta en los delitos cometidos para procurarse los medios para perpetrar los actos para los que Europol sea competente, los cometidos para facilitar o consumir la ejecución de los actos para los que Europol sea competente y los perpetrados para conseguir la impunidad de los actos para los que la Agencia sea competente.

Esta referencia a las competencias de Europol no puede cerrarse obviando las dos siguientes consideraciones: en primer lugar, que la cooperación policial no afecta a competencias estatales de orden público y seguridad interior de los Estados miembros, de modo que son las propias autoridades policiales nacionales las competentes para preservar el orden público y la seguridad interior dentro del territorio de sus Estados y las que deben aplicar las medidas coercitivas atendiendo a su propia legislación, de modo que la Agencia no puede ejercer poderes ejecutivos en los Estados miembros o en opinión de Marica (2012: 5) carece de competencia para llevar a cabo labores de vigilancia, seguimiento o en su caso para proceder a la detención de una persona ; y en segundo lugar, que son las propias autoridades policiales nacionales las que han de contactar con los órganos competentes de otros Estados miembros para investigar sobre hechos o personas puesto que Europol carece de competencias de investigación propias que recaen bajo el ámbito competencial propio de los Estados. Así pues, Europol se nos presenta como un órgano con poderes limitados en comparación con otras agencias o cuerpos de esta naturaleza como puede ser el FBI (Galetta *et al.*, 2016: 75).

Finalmente, y para ir cerrando esta aproximación al ámbito competencial de Europol, merece apuntar, asimismo, que conforme al art. 5.5 de la Decisión 2009/371, esta actúa como un organismo central contra la falsificación del euro con base en la Decisión 2005/511/JAI del Consejo, de 12 de

---

humanos; ciberdelincuencia; delitos contra la propiedad intelectual; o defraudación del IVA. Por su parte, el Reglamento Europol, en su anexo I, considera como formas de delincuencia algunas modalidades delictivas no contempladas en el anexo de la Decisión 2009/371, tales como, entre otras: el hurto con agravante, los abusos sexuales y la explotación sexual, y el genocidio, los crímenes de lesa humanidad y los crímenes de guerra.

julio de 2005, colaborando estrechamente con los Estados miembros de la UE, el Banco Central Europeo, la Comisión, la Oficina Europea de lucha contra el fraude (OLAF), Interpol y otros socios.

### III. EL TRATAMIENTO DE LA INFORMACIÓN COMO FORMA DE COOPERACIÓN

#### 1. EL PRINCIPIO DE DISPONIBILIDAD DE LA INFORMACIÓN

Sobre el tratamiento de la información<sup>24</sup> que, como hemos ya avanzado, constituye uno de los principales ejes de la actividad de Europol, cabe recordar que el Programa de Estocolmo titulado «Una Europa abierta y segura que sirva y proteja al ciudadano» ya insta a esta a convertirse en un eje para el intercambio de información entre las autoridades policiales de los Estados miembros<sup>25</sup>. Europol responde al objetivo de ayudar a los Estados miembros de la UE en la prevención y eliminación de las formas graves de delincuencia internacional; y, a *nivel práctico*, las principales tareas de Europol consisten en facilitar el intercambio de información entre los Estados miembros y proporcionar capacidad analítica. Un mandato que no podría materializarse si no se atiende al denominado *principio de disponibilidad*.

En este contexto, hemos de traer a colación el principio de disponibilidad, adoptado con el fin de mejorar, en general, la cooperación policial en el contexto de Europol y, en particular, la lucha contra el terrorismo y la delincuencia organizada y que se configura a modo de principio rector de la actividad de Europol, tal y como se desprende de la propia literalidad de la Decisión 2009/371<sup>26</sup>. Es en el Programa plurianual de la Haya, adoptado en el Consejo Europeo del 4 y 5 de noviembre de 2004, —en el que la Comisión fija las diez prioridades que hay que atender para reforzar el espacio europeo de Libertad,

---

<sup>24</sup> En adelante, cuando aludamos a la información, consideramos el término como aglutinador de información y/o inteligencia en el sentido descrito en el art. 2 de la Decisión Marco 2006/960 donde se considera *información y/o inteligencia*: todo tipo de información o datos en poder de los servicios de seguridad y, asimismo, todo tipo de información o datos en poder de autoridades públicas o entes privados, de la que puedan disponer los servicios de seguridad sin tener que acudir a la utilización de medidas coercitivas.

<sup>25</sup> Programa de Estocolmo que puede consultarse en DO C 115, de 4 de mayo de 2010.

<sup>26</sup> Considerando 10 de la Decisión 2009/371.

Seguridad y Justicia—<sup>27</sup>, donde aparece formulado el mencionado principio subrayando la necesidad de lograr un equilibrio entre la disponibilidad de la información y el respeto de los derechos fundamentales a la intimidad y a la protección de datos. En este se define por primera vez este principio de disponibilidad como un instrumento innovador del intercambio transfronterizo de información policial y se fija de forma categórica el 1 de enero de 2008 como la fecha a partir de la cual el intercambio de datos se basará en el mencionado principio.

Se trata de un principio que, aplicado en el ámbito territorial de la UE, implica, por un lado, que un funcionario de policía de un Estado miembro que necesite información para llevar a cabo sus funciones de investigación en el territorio de la UE pueda obtenerla de otro Estado miembro. Situados en este escenario, no hay que perder de vista que cualquier Estado miembro —por aplicación del principio de la disponibilidad—, además de acceder a la información a través de canales de intercambio como es la propia Europol, puede acceder a las bases de datos nacionales utilizadas por las fuerzas y cuerpos de seguridad de otro Estado miembro, lo que, como afirma Del Moral Torres (2010: 2), repercute positivamente sobre la cooperación y su utilidad policial.

Y, por otro lado, que el organismo policial del otro Estado miembro que posea dicha información la facilitará, es decir, la «pondrá a su disposición» para el propósito indicado, teniendo en cuenta el requisito de las investigaciones en curso en dicho Estado.

### 1.1. *El intercambio de información entre los servicios de seguridad españoles competentes y los servicios de seguridad competentes de otros Estados miembros*

Con el objetivo de regular la puesta en marcha y aplicación del principio de disponibilidad se adopta la Decisión Marco 2006/960/JAI —conocida como «iniciativa sueca»<sup>28</sup>— del Consejo, de 18 de diciembre de 2006, sobre la

<sup>27</sup> Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 10 de mayo de 2005, «Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia», COM (2005) 184 final, DO C 236 de 24 de septiembre de 2005); y Plan de Acción del Consejo y la Comisión por el que se aplica el Programa de La Haya sobre Refuerzo de la Libertad, la Seguridad y la Justicia en la UE Europea (Documento 2005/C 198/01, DOCE C 198, de 12 de agosto de 2005).

<sup>28</sup> Nombre que trae su origen en el hecho de que fue Suecia quien presentó, el 12 de octubre de 2005, la propuesta de Decisión Marco sobre el Intercambio de Información en

simplificación del intercambio de información entre los servicios de seguridad de los Estados miembros de la UE<sup>29</sup>, considerada la base de la cooperación policial en la UE. Así, la posibilidad de compartir información entre los Estados, en el ámbito policial, se torna en obligación al incluirse en un instrumento jurídicamente vinculante las condiciones en las que debe satisfacerse los requerimientos de información que provengan de los Estados miembros y que sea obtenida con anterioridad a la solicitud.

Esta decisión marco se incorpora a nuestro ordenamiento jurídico mediante la aprobación de la Ley 31/2010, de 27 de julio<sup>30</sup>. Como reiteradamente se ha señalado sobre este extremo, cabe destacar que resultan aplicables las disposiciones nacionales sobre protección de datos, lo que se traduce en la aplicación del estándar mínimo de protección fijado en el Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal —que entró en vigor para España el 1 de octubre de 1985— y, para los Estados que lo hayan ratificado, la prevista en su protocolo adicional, de 8 de noviembre de 2001, relativo a las autoridades de control y los tránsitos transfronterizos de datos. A ello hay que añadir, conforme al art. 6 de la citada ley, la necesidad de observar los principios de la Recomendación (87) 15 del Consejo de Europa.

Esta ley regula las normas que han de regir el intercambio de información<sup>31</sup> entre los servicios de seguridad españoles competente —a saber, las Fuerzas y Cuerpos de Seguridad del Estado, los Cuerpos de Policía de las Comunidades Autónomas y el Servicio de Vigilancia Aduanera— y los servicios de seguridad competentes de los demás Estados miembros. Y quedan excluidas del ámbito de aplicación de la Ley, en aplicación de su art. 1.3, los

---

virtud del principio de disponibilidad que se materializaría en la Decisión Marco del año 2006 (COM (2005) 490 final, de 12-10-2005).

<sup>29</sup> DOUE L 386/89, de 29 de diciembre de 2006.

<sup>30</sup> Ley 31/2010, de 27 de julio, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la UE, BOE núm. 182, de 28 de julio de 2010. Véase, asimismo, la Ley Orgánica 6/2010, de 27 de julio, complementaria de la Ley 31/2010 por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, BOE núm. 182, de 28 de julio de 2010.

<sup>31</sup> Tal y como hemos avanzado, cuando nos referimos a información estamos considerando incluido el concepto de *inteligencia* que, en virtud del art. 2 de la Ley 31/2010, abarca lo siguiente: «a) Todo tipo de información o datos en poder de los servicios de seguridad. b) Todo tipo de información o datos en poder de autoridades públicas o entes privados, de la que puedan disponer los servicios de seguridad sin tener que utilizar medidas coercitivas definidas de acuerdo con la legislación española».

intercambios de información «[...] que lleve a cabo el Centro Nacional de Inteligencia en el ámbito de los Acuerdos Internacionales ratificados por el Reino de España en materia de protección mutua de la información clasificada y en el ámbito de las relaciones de cooperación y colaboración con servicios de inteligencia de otros países o de Organismos Internacionales para el mejor cumplimiento de sus objetivos».

El intercambio de información entre los servicios competentes de los Estados miembros se lleva a cabo a través de sistemas de tratamiento de la información o bases de datos nacionales y, en este sentido, la Ley 31/2010 regula tanto la solicitud de información como el suministro de esta —bien de oficio, bien a petición de los servicios de seguridad competentes de otros Estados miembros— por los servicios españoles de seguridad competentes a los servicios de seguridad competentes de otros Estados miembros. En relación a la finalidad por la que puede solicitarse información, puede afirmarse que, así lo preceptúa el art. 7.1 de la citada Ley, la solicitud se cursa al «efecto de descubrir, prevenir e investigar la comisión de un delito» y, consecuentemente, la información se suministra por los servicios españoles de seguridad competentes para llevar «a cabo una investigación criminal o una operación de inteligencia criminal» pudiendo estos imponer condiciones relativas a la notificación de los resultados de la investigación u operación de inteligencia criminal tal y como dispone el art. 9 de la Ley 31/2010. El hecho de que la solicitud o el suministro de información responda a esta finalidad concreta, se traduce en la práctica en el hecho de que debe garantizarse el eventual uso indebido que se haga de la información y de los datos personales (Martínez Pérez y Poza Cisneros, 2013: 422).

Debe señalarse que, tal y como se desprende de la literalidad de la Ley 31/2010, tanto la solicitud como el suministro de información por los servicios españoles de seguridad competentes debe someterse a las mismas condiciones que las impuestas a escala nacional. Una aseveración que implica, a modo de ejemplo, que, ante una solicitud de información por los servicios españoles de seguridad competentes a los servicios de seguridad competentes de otros Estados miembros, estos no estarán obligados a trasmitirla cuando la información se ha obtenido de otro Estado miembro o de un tercero, salvo que medie autorización del Estado que la proporcionó, pero que tampoco los servicios españoles tendrán que suministrarla si estos han accedido a la información de otro Estado miembro o de un tercer país si no media la autorización correspondiente; y, asimismo, que solo se exigirá autorización judicial para la transmisión o el suministro de información cuando para acceder a esta haya sido necesaria tal autorización, de modo que deben aplicarse los mismos

criterios que si se tratara de un asunto exclusivamente interno<sup>32</sup>. Una autorización que tendrán que otorgar los Juzgados Centrales de Instrucción de la Audiencia Nacional o, en el caso de situarnos ante un procedimiento judicial abierto, el propio órgano judicial que esté conociendo del procedimiento<sup>33</sup>.

Además, la Ley 31/2010 regula los plazos en los que ha de suministrarse la información distinguiendo según se trate de solicitudes urgentes, no urgentes y aquellos supuestos no catalogables en un caso ni en otro. Así, los servicios españoles de seguridad competentes deben responder a las solicitudes urgentes de información en un plazo de ocho horas pudiendo este prorrogarse hasta un máximo de tres días y a las no urgentes en el de una semana siempre que la información solicitada se encuentre en una base de datos a la que tenga acceso directo el servicio de seguridad, una previsión necesaria puesto que, como señala Del Moral Torres (2010:3), debe asegurarse que las bases de datos a las que acceden los servicios de policía nacionales se encuentren accesibles, centralizadas y en servicio veinticuatro horas al día durante siete días a la semana. Y, como prevé el art. 10.4, «en todos los demás casos, el servicio de seguridad español competente velará porque la información solicitada por el servicio de seguridad competente de otro Estado miembro se comunique en el plazo de catorce días».

Respecto a las estructuras nacionales de tratamiento e intercambio de información, parece deseable avanzar por la senda de la armonización de estas, siendo esencial la coordinación y la colaboración en aras a lograr un modelo eficaz. Siguiendo a Del Moral Torres (2010: 4-6), puede sostenerse que el modelo genérico de inteligencia criminal en el caso de los Estados se distribuye en cuatro niveles: «nivel táctico», «nivel operacional», «nivel estratégico nacional» y «nivel político nacional».

---

<sup>32</sup> Esta cuestión relativa al hecho de que las condiciones que se aplican al intercambio de información transfronteriza no sean más estrictas que las que se aplican a nivel nacional a las operaciones de intercambio de información viene a quedar acreditada en las conclusiones que se presentan al Consejo sobre la evaluación del cumplimiento que han dado los Estados miembros a la Decisión Marco 2006/960. Véase el documento del Consejo de la UE, de 14 de octubre de 2011, 13970/2/11 REV2 JAI 606, DAPIX 112, CRIMORG 142, ENFOCOL 298 y ENFOCUSTOM 95.

<sup>33</sup> Sobre este particular, resulta de interés la Ley Orgánica 6/2010, de 27 de julio, complementaria de la Ley 31/2010, de 27 de julio, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la UE, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE núm. 182, de 28 de julio de 2010).



## 1.2. *El intercambio de información con Europol*

Como hemos apuntado anteriormente, la Ley 31/2010 regula el intercambio de información entre un servicio de seguridad español competente y los servicios de seguridad competentes de los otros Estados miembros de la UE, pero ello no excluye el intercambio de información también con Europol, que conforma una especie de banco central de datos. A ello cabría añadir la posibilidad de que la propia Europol pueda solicitar el intercambio de información relativa a datos PNR que se regula en la Directiva (UE) 2016/681<sup>34</sup>. Son las unidades nacionales las encargadas de suministrar la información, de conformidad con la legislación nacional, a Europol —bien por propia iniciativa, bien por petición de la propia Europol— para ser buscada, almacenada, intercambiada y compartida; y, asimismo, para ser analizada o tratada. A este respecto cabe señalar que se utiliza una red de intercambio de información segura y fiable (SIENA<sup>35</sup>) entre los funcionarios de enlace, los analistas y los expertos con la que se pretende, como apunta Bosilca (2013: 17), reducir el nivel de desconfianza de los Estados miembros a cooperar en el intercambio de inteligencia e información operativa y estratégica en materia delictiva.

Para ir finalizando, realizaremos algunas consideraciones en particular, acerca del intercambio de información con Europol. Sobre este tema, cabe subrayar que, si bien es cierto que a Europol se le reconoce la facultad para crear y mantener otros sistemas de tratamiento de la información y de los datos<sup>36</sup>, en principio, este tratamiento se materializa a través del Sistema de Información de Europol (SIE) y de los ficheros de trabajo de análisis regulados en los arts. 11 y 14 de la Decisión 2009/371 respectivamente<sup>37</sup>. Ambos serán objeto de nuestra atención en las siguientes páginas.

---

<sup>34</sup> Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (DOUE núm. 119, de 4 de mayo de 2016).

<sup>35</sup> Téngase en cuenta que SIENA es un programa de intercambio de información policial que se está utilizando desde el 1 de julio de 2009 y que, principalmente, se ocupa de la protección de los datos y la confidencialidad cumpliendo sobre este particular todos los requisitos jurídicos.

<sup>36</sup> Así se desprende de la lectura del art. 10.2 y 3 de la Decisión 2009/317.

<sup>37</sup> Sobre los ficheros de trabajo de análisis, asimismo, puede consultarse la Decisión 2009/936/JAI, de 30 de noviembre de 2009, por la que se adoptan las normas de desarrollo aplicables a los ficheros de trabajo de análisis de Europol (DOUE, L325/4 de 11 de diciembre de 2009).

El SIE, cuya nueva versión se adoptó en el 2010<sup>38</sup>, debe ser gestionado atendiendo a las disposiciones contenidas en la Decisión Europol del año 2009<sup>39</sup> y mantenido por la propia agencia, quien asume la responsabilidad de su buen funcionamiento desde el punto de vista tanto técnico como operativo. Su función principal consiste en detectar las coincidencias entre los datos suministrados y posibilitar la cooperación entre los agentes competentes de los diferentes Estados a los efectos de prevenir y combatir la delincuencia transnacional. Una función que debe desarrollarse preservando la seguridad en el intercambio o transmisión de información, de modo que se fijan los denominados códigos de tratamiento que permiten a los Estados compartir información sensible en condiciones óptimas para la protección de los datos y la seguridad en su intercambio.

En cada Estado miembro es la unidad nacional la que se responsabiliza de la comunicación con el SIE, de modo que tal unidad nacional es el único órgano de conexión entre Europol y las autoridades competentes de los Estados parte. Para una estrecha colaboración entre Europol y las unidades nacionales de los Estados miembros se utilizan los canales de comunicación, así el Estado transmisor —el que aporta datos al SIE— transfiere los datos al Estado afectado —denominado *Estado interesado*— y, para hacer la transferencia de datos personales, es necesario respetar las normas y garantías impuestas por la legislación nacional del Estado transmisor. El Estado destinatario o interesado tiene que informar —siempre que su legislación lo permita— al Estado transmisor del uso realizado con la información, así como los resultados obtenidos. Es por ello que los datos personales, los ficheros o los documentos que Europol recibe de la unidad nacional de enlace de un Estado parte se devolverán al Estado suministrador de la información, se suprimirán o destruirán cuando esa información ya no sea necesaria para los fines para las que haya sido almacenada, y, en todo caso, se suprimirán tras el cierre de un fichero de trabajo de análisis (Carrera Hernández, 2003: 104). Se encuentra disponible en todas las lenguas oficiales de la UE y posibilita el almacenamiento, la búsqueda, la visualización y el enlace de la información relacionada con delitos de carácter transnacional.

---

<sup>38</sup> Con carácter previo a la reforma, el SIE tenía un contenido limitado y definido. En este sentido el art. 6.1 del Convenio Europol refiriéndose al SIE decía que tenía: «[...] un contenido limitado y definido con precisión, que permitirá una rápida consulta de la información existente en los Estados miembros y en EUROPOL».

<sup>39</sup> De forma principal las relativas a los plazos de conservación y supresión de los ficheros, a la responsabilidad en materia de protección de datos, a la rectificación y supresión de datos y a la seguridad de estos.

En cuanto a los ficheros de trabajo de análisis creados, como resulta obvio, con fines de análisis, conviene anotar que estos constituyen unidades de almacenaje, modificación y utilización de los datos referentes a los delitos que entran dentro del radio de acción de Europol en la medida en que sea necesario para que esta desempeñe sus funciones<sup>40</sup>. En tanto en cuanto nos situamos ante ficheros automatizados de datos personales, su creación exige una orden de creación en el que el director de Europol deberá hacer constar, entre otros extremos, la denominación del fichero, su objetivo, la categoría de personas sobre las que versen los datos, la naturaleza de los datos o los participantes en el grupo de análisis en el momento de crear el fichero<sup>41</sup>. Ahora bien, el consejo de administración tiene potestad para encomendar al director que modifique tal orden de creación o, incluso, que cierre el fichero<sup>42</sup>. El fichero de trabajo de análisis se almacenará durante un período máximo de tres años, pudiendo el director decidir su continuación durante un nuevo lapso temporal de tres años. En todo caso, esta prórroga siempre deberá estar justificada con base en el principio de necesidad, lo que significa que Europol deberá probar que la conservación del fichero resulta estrictamente necesaria para atender los objetivos para los que fue creado<sup>43</sup> y su cierre conlleva la destrucción del fichero sobre el argumento de que los datos dejan de ser útiles para atender a los fines para los que fueron almacenados.

Interesa tener en cuenta que, para Europol, trabajan más de cien de los mejores analistas de inteligencia criminal del mundo, que desarrollan su actividad con las herramientas más vanguardistas. Y debe constatarse que para cada proyecto de análisis se prevé la creación de un grupo de análisis en el que trabajan en estrecha colaboración: por un lado, analistas y otros miembros del personal de Europol designados por el director; y, por otro lado, funcionarios de enlace o expertos de los Estados miembros de donde proviene la información o afectados por el análisis efectuado<sup>44</sup>. Siendo ello así, hemos de consta-

---

<sup>40</sup> Art. 14.1 de la Decisión 2009/371.

<sup>41</sup> Art. 16 de la Decisión 2009/371.

<sup>42</sup> Art. 16.4 de la Decisión 2009/371. Además, téngase en cuenta que, también, es el consejo de administración quien elabora las normas de desarrollo que resultan aplicables a los ficheros de trabajo de análisis. Unas normas que estando referidas principalmente a la seguridad de los datos y al control interno de su utilización requieren del dictamen previo de la autoridad común de control y que son aprobadas por mayoría cualificada del Consejo tras consultar al Parlamento Europeo tal y como preceptúa el art. 14.1 *in fine* de la Decisión 2009/371.

<sup>43</sup> Art. 16.3 de la Decisión 2009/371.

<sup>44</sup> Art. 14.2 de la Decisión 2009/371.

tar que, asimismo, pueden ser invitados a participar en las actividades de un grupo de análisis, por ejemplo, Eurojust, OLAF, Frontex, CEPOL, terceros Estados o la Interpol.

Los analistas de Europol desarrollan esta actividad analítica bajo un doble formato: análisis operativos efectuados para identificar los *cabos sueltos* existentes en las investigaciones transfronterizas en curso de la UE llevadas a cabo sobre operaciones delictivas y análisis estratégicos de carácter general que convierten a Europol en una pieza clave en el proceso de formulación de políticas. Y los documentos de análisis estratégicos se dividen en cuatro grupos:

1. La OCTA: el documento de análisis estratégico más importante elaborado por Europol que en el 2013 fue sustituido por la SOCTA. Se trata de un informe-evaluación de la amenaza de la delincuencia grave y organizada elaborado por Europol.
2. La TE-SAT: a través de la cual Europol elabora informes anuales sobre la situación y las tendencias del terrorismo en la UE en los que se informa al Parlamento Europeo y al Consejo del fenómeno del terrorismo en la UE desde el prisma de la actuación policial.
3. La ROCTA: un informe sobre la evaluación de la amenaza de la delincuencia organizada rusa puesto en marcha en 2008.
4. La OCTA-WA: un informe sobre la evaluación de la amenaza de la delincuencia organizada en África Occidental puesto en marcha en 2009.

Para ir cerrando esta parte dedicada al estudio del SIE y los ficheros de trabajo de análisis, cabe señalar que el espectro de personas sobre las que pueden versar los datos que se contienen en uno y otro sistema es más amplio en el supuesto de los ficheros de trabajo de análisis. Así pues, en ambos casos pueden incorporarse datos tanto sobre personas sospechosas, de conformidad con el derecho nacional, de haber cometido o de haber participado en un delito competencia de Europol o condenadas por este tipo de delito como acerca de personas sobre las que existan indicios concretos o motivos razonables, de acuerdo con el derecho nacional, para presumir que cometerán delitos competencia de la Agencia<sup>45</sup>. Aunque, en el caso de los ficheros de trabajo de análisis, los datos pueden referirse, además y entre otras, a personas sobre las que con-

---

<sup>45</sup> Así se desprende de la lectura de los arts. 12.1 y 14.1.a) de la Decisión 2009/371.

curre la condición de testigos, víctimas, intermediarios o acompañantes del infractor<sup>46</sup>.

Dicho esto, resulta oportuno para una adecuada contextualización de cómo se lleva a cabo el tratamiento de la información aludir, siquiera telegráficamente, a la llamada función de índice prevista en el art. 15 de la Decisión 2009/371. Europol elabora una función de índice de los datos almacenados en los ficheros de trabajo de análisis cuyo acceso está muy limitado. En concreto, la función de índice podrá ser consultada por el director, los directores adjuntos, el personal de Europol habilitado a tales efectos, los funcionarios de enlace y los miembros de las unidades nacionales debidamente habilitados. Esta función de índice que, como acabamos de avanzar, solo puede ser consultada por ciertas autoridades permite precisar si una información está almacenada en un fichero de trabajo de análisis, pero no cotejar o deducir el contenido de la información. Así pues, su objetivo es indicar con claridad a la persona que lo utilice si un fichero de trabajo de análisis contiene información que resulte útil o interesante para la realización de investigaciones o tareas que afectan a quien lo consulta. Llegados a este punto, conviene apuntar que nos situamos ante un detalle agregado al SIE no debiendo ser considerada la función de índice como una parte integrante de la base de datos de Europol.

En todo caso, para ir finalizando, conviene subrayar que el principio de disponibilidad no es absoluto lo que se traduce en la posibilidad de negar el acceso a la información en determinados supuestos. Así, por ejemplo, los servicios españoles de seguridad competentes podrán negarse a facilitar información que pudiera: perjudicar intereses esenciales en materia de seguridad nacional; comprometer el éxito de una investigación en curso o de una operación de inteligencia criminal o la seguridad de las personas: o ser claramente desproporcionada o irrelevante para el fin perseguido<sup>47</sup>. En suma, el principio analizado no implica el reconocimiento de un *cheque en blanco* que permita obtener y exija suministrar o facilitar información siempre y en todo caso. Así lo demuestra el hecho de que, tal y como se recoge en el art. 1 de la Decisión Marco 2006/960 y a título meramente ejemplificativo, ni existe por parte de los servicios de seguridad competentes de los Estados miembros la obligación de recoger y almacenar información con el propósito de facilitarla a los servicios de seguridad de otro Estado parte requirente ni la obligación de obtenerla mediante medidas coercitivas.

<sup>46</sup> Arts. 14.1. b), c), d) y e) de la Decisión 2009/371.

<sup>47</sup> Art. 11 de la Ley 31/2010.

## 2. LA CONFIDENCIALIDAD DE LA INFORMACIÓN

Tal y como hemos adelantado, el principio de disponibilidad responde al objetivo de asegurar que «los servicios de seguridad de los Estados miembros puedan intercambiar de forma rápida y eficaz la información e inteligencia disponibles para llevar a cabo investigaciones criminales u operaciones de inteligencia criminal»<sup>48</sup>. En todo caso, tal objetivo no puede suponer menoscabo alguno de los principios en los que se fundamenta la cooperación policial en la UE. A saber, el respeto de los derechos humanos, las libertades fundamentales y el Estado de Derecho y, en particular, la tutela del derecho fundamental a la protección de datos personales. Por esta razón se prevé que tanto Europol como el Estado que hace el correspondiente requerimiento y recibe la información deben preservar un nivel adecuado de protección de datos. Así pues, toda la información recopilada por Europol o que se intercambie a través de esta debe responder a un determinado nivel de protección según la clasificación que se haga de la misma que sea capaz de preservar las informaciones confidenciales.

En este sentido, se prevé el principio de confidencialidad que se regula en los arts. 40 y 41 de la Decisión 2009/371 y que encuentra su desarrollo en la Decisión 2009/968 por la que se adoptan las normas sobre confidencialidad de la información que se recopile en Europol o se intercambie con Europol<sup>49</sup>. Así, hablar de *confidencialidad* significa tratar las distintas medidas o normas de seguridad a las que está sometida toda la información tratada por o a través de Europol, para lo que resulta esencial el manual de seguridad aprobado por el consejo de administración, previa consulta al comité de seguridad. Recordemos que, como regla general, la unidad nacional es el único órgano de enlace entre Europol y las autoridades competentes de los Estados, de modo que esta es el canal por donde fluye la información en sentido bidireccional.

Con carácter previo al análisis de los diversos niveles de protección de los datos en función de los niveles de clasificación de Europol, realizaremos unas breves consideraciones relativas a la naturaleza de los datos. Siguiendo a Gacitúa Espósito (2014: 222), cabe decir que estos deben estar directamente relacionados con tales personas —apellido, apellido de soltera, nombre, alias o nombre falso utilizado, nacionalidad o número de la seguridad social— y con

---

<sup>48</sup> Art. 1 de la Decisión Marco 2006/960 que se complementa por la Decisión Marco 2008/977 del Consejo de 27 de noviembre de 2008 relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO L350 de 30 de diciembre de 2008).

<sup>49</sup> DOUE L332/17, de 17 de diciembre de 2009.

los delitos por estos cometidos<sup>50</sup>. Además, se pueden almacenar, tratar, modificar y utilizar ciertas «indicaciones»<sup>51</sup> con relación a personas condenadas o sospechosas de haber cometido o participado en algún delito competencia de Europol.

Así pues, queda prohibido el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical y asuntos relacionados con la salud<sup>52</sup> o la vida sexual salvo, siguiendo el tenor literal de la Decisión 2009/371, «cuando sea estrictamente necesario para la finalidad del fichero de que se trate y a menos que tales datos completen otros datos personales introducidos en ese mismo fichero»<sup>53</sup>. En este contexto, Wilson (2010) expone que las transferencias e intercambios de datos atienden a los niveles de riesgo de la privacidad. A pesar de que su estudio se refiere a la práctica clínica, en el ámbito de la confidencialidad tiene cierta analogía, ya que Europol trata con datos personales que deben de ser resguardados, pues su conocimiento, más allá de para lo que fueron creados, puede perjudicar a las personas. En este sentido, podemos encontrar investigaciones donde la información obtenida, probablemente, con un alto nivel de esfuerzo e inversión de recursos, al perder la privacidad podría obstaculizar la continuidad de la investigación para obtener los objetivos trazados<sup>54</sup>.

Llegados a este punto, resulta preciso distinguir diversos niveles de protección de los datos tratados por Europol o a través de Europol, de modo que, en función del nivel de clasificación de la información —elegido por el Estado

---

<sup>50</sup> Un elenco completo de la tipología de datos que pueden incorporarse lo encontramos en el art. 12.2 de la Decisión 2009/371.

<sup>51</sup> «Indicaciones adicionales» son, siguiendo el art. 12.3 de la Decisión 2009/371, los datos relativos a delitos, hechos imputados, fecha y lugar de comisión; medios utilizados o que puedan serlo; servicios responsables del expediente y número de referencia de este; sospecha de pertenencia a una organización delictiva; y condenas siempre que se refieren a delitos competencia de Europol.

<sup>52</sup> Véase por analogía el *Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME)*, Grupo de Trabajo sobre Protección de Datos del art. 29, doc. 00323/07/ES, adoptado el 15 de febrero de 2007.

<sup>53</sup> Arts. 10.3 y 14.1.e) de la Decisión 2009/371.

<sup>54</sup> Un ejemplo de este tipo de investigaciones lo encontramos en las actuaciones de Europol en la lucha contra el tráfico de seres humanos. Véase Europol, *Europol supports successful operation against human trafficking network*. Disponible en: <https://www.europol.europa.eu/content/europol-supports-successful-operation-against-human-trafficking-network>

miembro que suministra la información a Europol o por la propia agencia<sup>55</sup>—, se establecerán diferentes medidas de seguridad que habrán de respetarse tanto en Europol como en los Estados miembros<sup>56</sup>. Lógicamente, queda al margen de tales niveles de protección solo aquella información catalogada como pública, de modo que sobre el resto de información los Estados miembros deben garantizar un nivel básico de protección que incluye la obligación de reserva y confidencialidad sobre esta<sup>57</sup>.

En este sentido, es inevitable traer a colación la Directiva (UE) 2016/680 referente 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 resulta aplicable<sup>58</sup>. Esta directiva prevé que los Estados miembros deberán «proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales»<sup>59</sup>. De esta forma, la autoridad responsable del tratamiento de los datos debe tener en cuenta, en primer lugar, los acuerdos de cooperación celebrados con Europol que permitan el intercambio de datos personales al llevar a cabo la evaluación de todas las circunstancias que concurran en la transferencia de datos<sup>60</sup>. Y, en segundo lugar, si la transferencia de datos va a estar sujeta a obligaciones de confidencialidad y al principio de especificidad, que garantiza que los datos no se tratarán para fines distintos de aquellos para los que se han transferido<sup>61</sup>.

<sup>55</sup> Art. 11 de la Decisión 2009/968.

<sup>56</sup> Véase el anexo de la Decisión 2009/968 donde se establecen los niveles de clasificación Europol y el cuadro de equivalencias entre los Estados miembros de los niveles de clasificación de la información.

<sup>57</sup> Art. 10.2 de la Decisión 2009/968.

<sup>58</sup> DO L 119/89, de 4 de mayo de 2016.

<sup>59</sup> Art. 1.2. a) de la Directiva (UE) 2016/680.

<sup>60</sup> Considerando (71) de la Directiva (UE) 2016/680. Un ejemplo es el caso de la transferencia de datos PNR. El art. 10.2 de la Directiva (UE) 2016/681 indica que «Europol podrá dirigir, caso por caso, a la Unidad de Información de Pasajeros (UIP) de cualquier Estado miembro, a través de la unidad nacional de Europol, una solicitud electrónica debidamente motivada de transmisión de datos PNR específicos o del resultado del tratamiento de los mismos». Así pues, dicha solicitud señalará las causas razonables por las que Europol considera que la transmisión de los datos PNR o de los resultados de su tratamiento va a ayudar a prevenir, detectar o investigar la infracción penal en cuestión.

<sup>61</sup> Arts. 4.1 f) y 35 de la Directiva (UE) 2016/680.



Así, cuando además de ese nivel básico de protección sea necesario adoptar medidas de seguridad adicionales, la información estará sometida a un nivel de clasificación de Europol. Pueden distinguirse las siguientes categorías: Europol Restricted (Europol difusión limitada), Europol Confidential (Europol confidencial), Europol Secret (Europol reservado) y Europol Top Secret (Europol Secreto)<sup>62</sup>.

El nivel Europol Restricted (Europol difusión limitada) abarca solo la información y el material cuya revelación<sup>63</sup> no autorizada podrá resultar desfavorable para los intereses esenciales de Europol, de la UE o de uno o varios Estados miembros. Nos situamos ante el nivel básico de la clasificación, de modo que la información clasificada como Europol difusión limitada se refiere a datos de carácter personal relativos a personas sospechosas de haber cometido o haber participado en un delito de la competencia de Europol y, también, a datos referentes a personas condenadas por tal delito. Por su parte, se clasifica como Europol Confidential (Europol confidencial) aquella información y material cuya revelación no autorizada puede causar un perjuicio a los intereses esenciales de Europol, de la UE o de uno o varios Estados miembros. Así las cosas, nos situaríamos en el nivel medio en cuanto a las medidas de seguridad para preservar la información. En un tercer nivel, situamos la información que puede clasificarse de Europol Secret (Europol reservado) y que se aplica a la información y al material cuya revelación no autorizada puede causar un perjuicio grave para los intereses esenciales de Europol, de la UE o de uno o varios Estados miembros. En este caso —nivel alto de seguridad de la información—, el perjuicio se cataloga como grave. Este nivel de seguridad se aplica tanto a información económica y financiera como a los datos sobre el comportamiento. Y, finalmente y en un cuarto nivel, se sitúa Europol Top Secret (Europol Secreto), que alude al más alto nivel de seguridad que se puede aplicar a los datos de Europol. En particular, este nivel de seguridad se aplica a información y material cuya revelación no autorizada puede causar un perjuicio excepcionalmente grave a los intereses esenciales de Europol, de la UE o de uno o varios Estados miembros. En este sentido, gozan del más alto nivel de seguridad, entre otras, las siguientes categorías de datos: los que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, los datos referentes a la vida sexual o a la salud, información sobre identificación forense como impresiones dactilares, resultados de la evaluación del ADN, caracteres de la voz, grupo sanguíneo, infor-

<sup>62</sup> Art. 10.4 de la Decisión 2009/968.

<sup>63</sup> *Revelar* se entiende como hacer visible o descubrir la información sin que sea necesario que se llegue hasta el punto de su difusión.

mación dental y datos con respecto a las víctimas o posibles víctimas, testigos o posibles testigos (Marica, 2012: 29).

#### IV. CONSIDERACIONES FINALES

El marco general en el que se encuadra el presente estudio se centra en el tratamiento e intercambio de la información —que resulta clave para garantizar una eficaz cooperación policial en la lucha y erradicación de la delincuencia transnacional y el terrorismo— llevado a cabo por Europol o a través de Europol.

El tratamiento de la información permite a esta Agencia Europea de Policía articular una respuesta más eficaz y eficiente ante los eventuales riesgos que amenazan las necesidades securitarias de la UE. Ahora bien, es necesario buscar un adecuado equilibrio a fin de evitar que ese afán securitario vaya en detrimento de los principios que inspiran el Estado de Derecho en los que se basa la UE. La mayor seguridad o el afán de incrementar la eficacia policial en la lucha contra el terrorismo y la delincuencia transfronteriza no debe suponer, en general, menor protección de los derechos humanos y las libertades individuales y, en particular, merma del derecho a la intimidad y a la protección de los datos personales.

En este contexto, el tratamiento de la información ha sido abordado desde la perspectiva de las autoridades competentes estatales lo que ha exigido el estudio del principio de la disponibilidad de la información y del principio de confidencialidad, sobre los que podemos avanzar las siguientes reflexiones.

El principio de la disponibilidad de la información se articula jurídicamente a través de la Decisión Marco 2006/960/JAI, una norma que se incorpora al ordenamiento jurídico interno a través de la Ley 31/2010 que regula el intercambio de información entre un servicio de seguridad español competente y los servicios de seguridad competentes de los otros Estados miembros de la UE, así como el intercambio con la propia Europol.

En virtud de este principio, los Estados están obligados a satisfacer los requerimientos de información que provengan de los demás Estados miembros. Conviene, no obstante, matizar que la disponibilidad no implica expedir un *cheque en blanco* que permita obtener y exija suministrar información siempre y en todo caso.

No resulta exagerado sostener que su puesta en marcha innova el intercambio transfronterizo de información policial. De hecho, se puede aseverar que el principio de disponibilidad constituye un punto de inflexión en las posibilidades de compartir información mediante el cual se apuesta por la

simplificación y eficiencia en su intercambio a los efectos de llevar a cabo investigaciones criminales u operaciones de inteligencia criminal.

Por todo ello, es necesario someter el funcionamiento y la aplicación de este principio a condiciones rigurosas por lo que respecta a la protección de los datos, máxime si tenemos en cuenta el carácter excesivamente generalista del Convenio 108 para salvaguardar de forma efectiva la protección de los datos en el ámbito de la cooperación policial. Todo ello se traduce en la aceptación del principio de disponibilidad sobre la base de un sistema adecuado de protección de datos capaz de preservar un estándar alto y equivalente de protección de estos. En materia de protección de datos, en el contexto que estamos analizando, el estándar mínimo de protección lo fija el Convenio 108. Y, asimismo, debe tenerse en consideración la Recomendación (87) 15, adoptada por el Consejo de Ministros del Consejo de Europa, que desarrolla y modula el Convenio 108 en función del contexto policial, de modo que esta recomendación regula el uso de datos personales en el ámbito policial convirtiéndose tras su incorporación a Europol en el estándar de protección de los datos en los tratamientos de datos personales efectuados con fines policiales. En fin, la citada recomendación que conforma un «texto de mínimos» incorpora los criterios de protección uniformes en los Estados miembros de modo que cada Estado debe garantizar que su derecho interno ofrezca un nivel de protección de los datos como mínimo equivalente al del Convenio 108. Llegados a este punto, puede sostenerse que el estándar de garantía de los datos va a ser directamente el mínimo común que representan esos instrumentos internacionales.

Por lo que respecta al principio de la confidencialidad —regulado en la Decisión 2009/371 que es desarrollada por la Decisión 2009/968 y que serán derogadas por el Reglamento 2016/794—, es necesario advertir que este nos pone sobre la pista de las distintas medidas o normas de seguridad a las que está sometida toda la información tratada por o a través de Europol. De modo que existen diversos niveles de protección de los datos en función de los niveles de clasificación de la información. Como regla general, queda prohibido el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical o los relacionados con la salud o la vida sexual. A ello hay que añadir que solo la información catalogada como pública queda al margen de los mencionados niveles de protección; y es sobre el resto de información sobre la que los Estados miembros deben garantizar un nivel básico de protección que incluye la obligación de reserva y confidencialidad sobre esta.

Una última observación que no debemos pasar inadvertida respecto al principio de la confidencialidad consiste en que cuando además del nivel básico de protección sea necesario adoptar medidas de seguridad adicionales,

la información se someterá a un nivel de clasificación de Europol. Así pueden distinguirse entre las categorías de Europol difusión limitada, Europol confidencial, Europol reservado y Europol secreto. Unas categorías que se establecen en función de si la información puede resultar desfavorable, puede causar un perjuicio, puede causar un perjuicio grave o un perjuicio excepcionalmente grave a los intereses esenciales de Europol, de la UE o de uno o varios Estados miembros.

Para finalizar, podemos sostener que parece indiscutible el peligro que implica el tratamiento de la información en el seno de la cooperación policial por lo que es necesario articular las garantías jurisdiccionales necesarias para preservar el derecho a la protección de datos evitando intromisiones ilegítimas a la par que se logra el adecuado y nada fácil equilibrio entre libertad y seguridad. Un concepto este último que, aunque se caracteriza por su elasticidad, siempre ha de respetar el límite del contenido esencial del derecho a la protección de datos. En suma y como conclusión final, cabe sostener que resulta clave lograr en cada caso la mencionada ponderación de los intereses en juego —fines de la cooperación policial y el bien jurídico protegido por el derecho a la protección de datos— para conseguir el necesario y complicado equilibrio entre seguridad y libertad.

### *Bibliografía*

- Bonn, M. (2007). El Programa de la Haya. El Espacio de Libertad, Seguridad y Justicia en la Unión Europea. En L. Arroyo Zapatero y A. Nieto Martín (dirs.). *El derecho penal de la Unión Europea. Situación actual y perspectivas de futuro* (pp. 29-36). Cuenca: Universidad de Castilla-La Mancha.
- Bosilca, R. L. (2013). Europol and counter terrorism intelligence sharing. *Europolity*, 7, 7-19.
- Carrera Hernández, F. J. (2003). *La cooperación policial en la Unión Europea: Acervo Schengen y Europol*. Madrid: Colex.
- De Moor, A. (2010). The Europol Council Decision: Transforming Europol into an Agency of the European Union. *Common Market Law Review*, 47, 1089-1121.
- Del Moral Torres, A. (2010). La cooperación policial en la Unión Europea: propuesta de un modelo europeo de inteligencia criminal. *Análisis del Real Instituto Elcano*, 50, 1-12.
- Gacitúa Espósito, A. L. (2014). *El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea (en busca del equilibrio entre la libertad y la seguridad)*. Barcelona: Universidad Autónoma de Barcelona.
- Galleta, A., Kloza, D. y De Hert, P. (2016). *Cooperation among data privacy supervisory authorities by analogy: lessons from parallel European mechanisms*. Brussels, etc.: Phaedra II.
- Marica, A. (2012). El sistema de tratamiento de la información en Europol. *Working papers*, 309, 1-30.

- Martínez Pérez, F. y Poza Cisneros, M. (2013). El principio de disponibilidad: antecedentes penales y convenio de Prüm. En A. Arnaiz Serrano (coord.). *Cooperación judicial penal en Europa* (pp. 417-496). Madrid: Universidad Carlos III de Madrid, Instituto de Justicia y Litigación Alonso Martínez
- Niemeier, M., y Wiegand, M. A. (2010). Europol and the architecture of internal security. En J. Monar (dir.). *The institutional dimension of the European Union's area of freedom, security and justice* (pp. 169-194). Lang, Brussels, New York: P. I. E. Peter Lang.
- Nunzi, A. (2007). European police office: Europol. En *Le droit pénal de l'Union européenne. The European Union criminal law* (pp. 285-292). Ramonville-Saint-Agne: Erès.
- Pérez Gil, J. (2007). Actuación policial concertada más allá de las fronteras: los equipos conjuntos de investigación en la UE. *Revista de Estudios Europeos*, 45, 65-79.
- Wilson, T. (2010). Information sharing: an exploration of the literature and some propositions. *Information Research: An International Electronic Journal*, 15. Disponible en: <http://InformationR.net/ir/15-4/paper440.html>.