

**W**

**WORKING  
PAPERS**

**309**

**El sistema de tratamiento de la información  
en EUROPOL**

**ANDREEA MARICA**



*Institut de Ciències Polítiques i Socials*  
Adscrit a la Universitat Autònoma de Barcelona



## **El sistema de tratamiento de la información en EUROPOL**

ANDREEA MARICA  
Universidad Carlos III de Madrid

WP núm. 309  
Institut de Ciències Polítiques i Socials  
Barcelona, 2012

El Institut de Ciències Polítiques i Socials (ICPS) es un consorcio creado en 1988 por la Diputación de Barcelona y la Universitat Autònoma de Barcelona, institución esta última a la que está adscrito a efectos académicos.

“Working Papers” es una de las colecciones que edita el ICPS, previo informe del correspondiente Comité de Lectura, especializada en la publicación -en la lengua original del autor- de trabajos en elaboración de investigadores sociales, con el objetivo de facilitar su discusión científica.

Su inclusión en esta colección no limita su posterior publicación por el autor, que mantiene la integridad de sus derechos.

Este trabajo no puede ser reproducido sin el permiso del autor.



Edición: Institut de Ciències Polítiques i Socials (ICPS)  
Mallorca, 244, pral. 08008 Barcelona (España)  
<http://www.icps.cat>

© Andreea Marica

ISSN: 1133-8962  
DL: B-10186-2012

## **LA OFICINA EUROPEA DE POLICÍA: EUROPOL**

Las actividades de prevención y represión de las formas de delincuencia organizada grave exigen un planteamiento común para llegar a mejores resultados que los de las actividades individuales de los Estados Miembros” (Bonn, 2007: 34). Por lo tanto, en la lucha contra la delincuencia organizada, la Oficina Europea de Policía (en adelante EUROPOL) se define como uno de los actores principales, siendo la Agencia de seguridad de la UE que gestiona la información y que nació como consecuencia de la ampliación de la libre circulación de personas que se vio unida al desarrollo de los fenómenos de la delincuencia organizada a nivel internacional, originando la necesidad de establecer una mayor cooperación entre los Estados en la lucha para combatir este fenómeno delictivo.

La base jurídica de EUROPOL fue el Acto del Consejo de 26 de julio de 1995 (en vigor desde el 1 de octubre de 1998) y empezó a desplegar sus funciones a partir del 1 de julio de 1999. Su antecedente más cercano fue la Unidad de Drogas de EUROPOL, que inicio sus actividades de forma limitada el 3 de enero de 1994. Recientemente, el Convenio EUROPOL se vio sustituido por la Decisión del Consejo de 6 de abril de 2009, mediante cual a la Oficina de Policía Europea se le asigna el estatuto de Agencia de la Unión Europea, de naturaleza similar a EUROJUST o la CEPOL.

La definición de quién o qué es EUROPOL, la podríamos formular partiendo quizá de su objetivo clave, que consiste en apoyar y reforzar las acciones de las autoridades competentes de los Estados miembros, así como en mejorar el marco de la cooperación entre los mismos, en materia de prevención y lucha contra la delincuencia organizada, el terrorismo, el tráfico ilícito de estupefacientes, el tráfico de seres humanos, las redes de inmigración clandestina, el tráfico ilícito de materias radioactivas y nucleares, el tráfico ilícito de vehículos, la lucha contra la falsificación del euro, el blanqueo de dinero vinculado con las actividades delictivas internacionales<sup>1</sup>, y otras formas de delitos graves que afectan a dos o más Estados miembros.

---

<sup>1</sup> Tras las modificaciones con respecto a la competencia de EUROPOL, éstas han sido ampliadas ofreciendo de esta forma la posibilidad de encargarse de todos los delitos graves, incluso los delitos contra la vida, la integridad física, la integridad física y la libertad de los sujetos: homicidio voluntario; agresión con lesiones graves; tráfico ilícito de órganos y tejidos humanos; secuestro; retención ilegal; racismo y xenofobia; delitos contra la propiedad y los bienes públicos; delitos de fraude: robos organizados y ataques organizados; tráfico ilícito de bienes culturales, incluidos las antigüedades y las obras del arte; fraude y estafa; chantaje y extorsión de fondos; violación de derechos de la propiedad industrial; falsificación de mercancías; falsificación de documentos administrativos; tráfico de documentos falsos; falsificación de moneda y medios de pago; delito informático; corrupción; comercio ilegal; delitos contra el medio ambiente; tráfico ilícito de armas, municiones y explosivos; tráfico ilícito de animales protegidas por la ley; tráfico ilícito de especies y esencias vegetales protegidas por la ley; delitos contra el medio ambiente y tráfico ilícito de sustancias hormonales y otros factores de crecimiento. Algunos delitos competencia de EUROPOL tienen la definición expresamente ofrecida por el anterior Convenio EUROPOL: delitos relativos al tráfico ilícito de estupefacientes y sustancias psicotrópicas; blanqueo de capitales; tráfico ilícito de material nuclear y radioactivo; inmigración clandestina; trata de seres humanos y tráfico de vehículos robados. La principal dificultad práctica que puede encontrarse en relación con la competencia material de EUROPOL deriva de la existencia de una pluralidad de códigos penales nacionales y, en consecuencia, de diferentes definiciones y tipificaciones de algunos delitos competencia de EUROPOL.

En este caso, podríamos considerar a esta Agencia como una especie de oficina de asesoramiento y apoyo a los servicios policiales nacionales, encargada de recoger, intercambiar, transmitir y analizar datos e información, teniendo la capacidad de profundizar en determinados conocimientos especializados, proporcionando datos estratégicos y elaborando informes, siempre a partir de los datos aportados por los servicios competentes de los diferentes Estados miembros<sup>2</sup>.

Ahora bien, para alcanzar los objetivos arriba mencionados, EUROPOL colaborará con los Estados miembros facilitando el intercambio de información, desempeñando funciones de recogida, compilación y análisis de información y datos, y en consecuencia llevará a cabo Análisis Operativos<sup>3</sup> y Estratégicos (Informes Estratégicos<sup>4</sup>), como también aportará su experiencia y colaboración técnica en las investigaciones<sup>5</sup> y actuaciones efectuadas en el marco de la Unión Europea. Las investigaciones quedarán bajo responsabilidad jurídica del Estado miembro en el que tiene lugar la actividad.

Hay que subrayar que el análisis de la información o, dicho de otra manera, el análisis de inteligencia, es la piedra angular de todas las actividades modernas basadas en la información y por lo tanto es crucial para todas las operaciones efectuadas por EUROPOL. Por lo tanto, en cuanto a los Análisis Operativos de EUROPOL, el objetivo de éstos consiste en facilitar la información destinada a las operaciones en curso en los Estados miembros de la UE, ayudando a identificar los llamados “cabos sueltos” de una operación delictiva.

Es imprescindible subrayar que los sistemas de EUROPOL están interconectados, lo que conlleva a que toda la información introducida en uno de ellos se puede identificar también en los demás<sup>6</sup>. Ahora bien, en cuanto a los documentos de Análisis Estratégico de EUROPOL, en función del ámbito delictivo analizado, éstos se dividen en cuatro grupos:

- 1) OCTA: informe-evaluación de la amenaza de la delincuencia organizada, puesto en marcha en 2006;

---

<sup>2</sup> Panorama de EUROPOL, Informe general sobre las actividades de EUROPOL, editado por la Oficina Europea de Policía, 2011.

[https://www.europol.europa.eu/sites/default/files/publications/es\\_europolreview.pdf](https://www.europol.europa.eu/sites/default/files/publications/es_europolreview.pdf)

<sup>3</sup> El análisis operativo es el más práctico. Tiene como misión tratar de ver allí donde los investigadores no pueden ver por la cantidad de los datos y por su dispersión. Este análisis tiene como misión iniciar nuevas líneas de investigación a raíz de hallazgos en la información que no son fáciles de ver por aquello de que algunas veces los árboles no dejan ver claramente el bosque. Información ofrecida en la página web de EUROPOL.

<sup>4</sup> Al hablar sobre informes estratégicos nos referimos al ámbito que abarca los informes de situación, los análisis de tendencias y los informes –evaluación de la amenaza que se elaboran en el marco de EUROPOL.

<sup>5</sup> EUROPOL participará en calidad de apoyo en equipos conjuntos de investigación y podrá prestar asistencia en todas las actividades, así como intercambiar información con todos los miembros del equipo conjunto de investigación en el que participa sin poder tomar parte en la adopción de ninguna medida coercitiva (art. 6, Decisión del Consejo de 6 de abril de 2009 por la que se crea la Oficina Europea de Policía).

<sup>6</sup> EUROPOL pone de relieve que el análisis de las redes sociales aparece como una forma innovadora para analizar la información y apoyar investigaciones relevantes sobre la delincuencia organizada y el terrorismo.

- 2) TE-SAT: informe sobre la situación y las tendencias del Terrorismo en la UE, puesto en marcha en 2007;
- 3) ROCTA: informe-evaluación de la amenaza de la delincuencia organizada rusa, puesto en marcha en 2008;
- 4) OCTA-WA: informe-evaluación de la amenaza de la delincuencia organizada en África Occidental, puesto en marcha en 2009<sup>7</sup>.

Es imprescindible subrayar que EUROPOL aparece como un Banco Central de Datos (dado que el Banco Mundial de Datos es INTERPOL), que como hemos visto, no se limita a ser un mero transmisor y receptor de información de carácter criminal, sino que profundiza en los conocimientos especializados utilizados por los servicios competentes de los Estados miembros en el marco de sus investigaciones y proporciona asistencia técnica gozando de un Sistema Informático de Datos que consta de tres elementos: el sistema de información; los ficheros de trabajo y el sistema de índice.

Es importante subrayar que EUROPOL no tiene capacidad ejecutiva; dicho de otra forma, la Oficina Europea de Policía no tiene las altas competencias de las que gozan los órganos policiales nacionales: no puede efectuar vigilancias, seguimientos, intervenciones telefónicas, no tiene la posibilidad de detener y arrestar, etc. La única posibilidad que le haya sido conferida es la de trabajar con los datos que les suministran los Estados miembros. Sin embargo sus actividades refuerzan la eficacia de los Cuerpos Nacionales de Policía sabiendo que cada Estado miembro designa una Unidad Nacional<sup>8</sup>, siendo ésta el único órgano de enlace entre EUROPOL y los servicios competentes de los Estados miembros.

En concreto, la labor de EUROPOL se da más bien en el ámbito de la inteligencia y consiste en efectuar análisis operativos, informes de situación, análisis de tendencias, informes-evaluación de la amenaza, como también informes de situación y tendencias

---

<sup>7</sup> Panorama de EUROPOL, Informe general sobre las actividades de EUROPOL, editado por la Oficina Europea de Policía, 2011.

[https://www.europol.europa.eu/sites/default/files/publications/es\\_europolreview.pdf](https://www.europol.europa.eu/sites/default/files/publications/es_europolreview.pdf)

<sup>8</sup> Con respecto a las Unidades Nacionales, el art. 8 del Decisión del Consejo por la que se crea EUROPOL, prevé que: "1) Cada Estado miembro creará o designará una unidad nacional encargada de ejecutar las funciones enumeradas en el presente artículo. Se designará a un agente en cada Estado miembro como jefe de la Unidad Nacional. 2) La Unidad Nacional será el único órgano de enlace entre EUROPOL y los servicios competentes de los Estados miembros. No obstante, los Estados miembros podrán autorizar contactos directos entre las autoridades competentes designadas por EUROPOL en las condiciones que determine el Estado miembro de que se trate, incluida la participación previa de la Unidad Nacional. 3) Los Estados miembros adoptarán todas las medidas necesarias para asegurar la ejecución de las funciones de la unidad nacional y, en particular, el acceso de la unidad nacional a los datos nacionales pertinentes. 4) La función de las Unidades Nacionales será: 1) Suministrar por iniciativa propia a EUROPOL las informaciones y datos necesarios para el desempeño de las funciones de este organismo; 2) Responder a las solicitudes de información, de suministro de datos y de asesoramiento formuladas por EUROPOL; 3) Mantener al día sus informaciones y datos; 4) Con arreglo a las disposiciones del Derecho nacional, aprovechar las informaciones y los datos de interés para los servicios competentes y transmitirlos a los mismos; 5) Remitir a EUROPOL las solicitudes de asesoramiento, información, datos y análisis; 6) Transmitir a EUROPOL informaciones para su almacenamiento en sus bases de datos; 7) Velar por la legalidad de cada operación de intercambio de información con EUROPOL (...)."

basados en los datos que los Estados miembros, representados por las Unidades Nacionales y los Funcionarios de Enlace, los suministran directamente al Sistema de Tratamiento de la Información, en conformidad con su legislación nacional<sup>9</sup>.

## **SISTEMA DE TRATAMIENTO DE LA INFORMACIÓN**

El Sistema de Tratamiento de la Información es el sistema o la base electrónica donde están almacenados, tratados y analizados los datos enviados por los Estados miembros o aportados por los funcionarios de EUROPOL. En tanto que los objetivos fundamentales son recopilar e intercambiar información y facilitar la cooperación entre las autoridades policiales en su lucha contra la delincuencia organizada y el terrorismo y siendo además el proveedor de evaluación periódicas sobre las amenazas, la Agencia creará y gestionará un Sistema de Información de EUROPOL, así como Ficheros de Trabajo de Análisis.

### ***Sistema de información de EUROPOL***

Antes de la reforma de 2009 del estatuto jurídico de EUROPOL, su Sistema de Información<sup>10</sup> de Datos tenía un contenido limitado y definido, en el cual se podrían “almacenar, modificar y utilizar sólo los datos necesarios para el cumplimiento de las funciones de EUROPOL, con la excepción de los datos sobre delitos conexos<sup>11</sup>, siendo constituido con la intención de que permita una rápida consulta de la información almacenada y que haya sido proporcionada por los Estados miembros o por EUROPOL<sup>12</sup>.

En la Decisión del Consejo de 6 de abril de 2009 por la que se crea la Oficina Europea de Policía, cambia el sentido de la redacción, se elimina la limitación y se prevé expresamente la clase de datos<sup>13</sup> que serán introducidos en el Sistema de Información de

---

<sup>9</sup> Capítulo II, Sistemas de Tratamiento de la Información, Decisión del Consejo de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía.

<sup>10</sup> Se entenderá por Sistema de Información el “conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de los datos de carácter personal” (Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por el Real Decreto 994/1999, de 11 de junio, y publicado en el BOE de 25 de junio de 1999).

<sup>11</sup> El art. 8.1 del Convenio EUROPOL establecía que: “en el sistema de información sólo se podrán almacenar, modificar y utilizar los datos necesarios para el cumplimiento de las funciones de EUROPOL, con excepción de los datos sobre los delitos conexos de conformidad con el párrafo segundo del apartado 3 del artículo 2”.

<sup>12</sup> El art.6.1 del anterior Convenio EUROPOL establecía que el sistema de información de EUROPOL 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>13</sup> Literalmente, el art. 12 Decisión EUROPOL establece que: “El sistema de información de EUROPOL solo se podrá utilizar para tratar los datos necesarios para el cumplimiento de las funciones de EUROPOL. Los datos introducidos se refieren a: 1) Las personas que sean sospechosas, de acuerdo con el derecho nacional del Estado miembro de que se trate, de haber cometido o de haber participado en un delito que sea competencia de EUROPOL, o que hayan sido condenadas por tal delito; 2) Las personas respecto de las cuales existan indicios concretos o motivos razonables, de acuerdo con el Derecho nacional de cada Estado miembro de que se trate, para presumir que cometerán delitos que son competencia de EUROPOL”.



EUROPOL<sup>14</sup>. Es importante subrayar que estos datos deberán ser recogidos con fines determinados, explícitos y legítimos, adecuados, pertinentes y no excesivos en relación con los fines para los que se recaben y para los que se traten<sup>15</sup>.

Anteriormente, el Convenio EUROPOL<sup>16</sup> ampliaba quizá demasiado la posibilidad de que el Sistema pudiese abarcar, además de los datos expresamente mencionados, también “otras características útiles”. Todo esto conllevaba el riesgo de que se pudiesen almacenar también los datos personales especiales –nos referimos aquí a los llamados “datos sensibles”<sup>17</sup>–, que revelan el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, así como el tratamiento de los datos relativos a la salud o a la vida personal<sup>18</sup>.

Con la actual Decisión del Consejo (Decisión de EUROPOL), para no dejar lugar a duda, en el art. 10. 3 se prevé expresamente que queda prohibido el tratamiento de los datos personales que revelen el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas o la afiliación sindical, el tratamiento de datos relacionados con la salud o la vida sexual. En la medida en que sea necesario, el art. 12, ap. 2 letra g) de la Decisión permite que el contenido del Sistema de Información de EUROPOL abarque “otras características que puedan ser útiles” para la identificación de un sujeto y especifica cuáles serían éstas. En particular, según la Decisión, se trataría de los “rasgos físicos específicos, objetivos y permanentes, tales como los datos dactiloscópicos y el perfil del ADN (establecido a partir de la parte no codificante del ADN).

No obstante, tanto en el anterior Convenio EUROPOL<sup>19</sup>, así como en el nuevo

---

<sup>14</sup> Art. 12 de la Decisión del Consejo de 6 de abril de 2009 por la que se crea la Oficina Europea de Policía, 2009/371/JAI, DOUE L 121/37, 15.5.2009.

<sup>15</sup> Art. 4.1.a), Reglamento (CE), N. 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales para las instituciones y los organismos comunitarios y a la libre circulación de estos datos, DO L 8/ 12.1.2001.

<sup>16</sup> Convenio EUROPOL, art. 8, ap. 2, punto 5.

<sup>17</sup> Datos personales: toda información sobre una persona física identificada o identificable; se considerará identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. COM(2005) 475 final.

<sup>18</sup> Acto del Consejo de 3 de noviembre de 1998 por el que se aprueban las normas aplicables a los ficheros de análisis de EUROPOL, art.6, letras d),e) y f) que prevén explícitamente que los ficheros de trabajo de análisis abarcan datos con respecto a la profesión y captaciones del sujeto, es decir datos con respecto a su actividad laboral y profesional actual y anterior, los títulos académicos obtenidos, las aptitudes que tiene el sujeto así como las captaciones y otros conocimientos. Aun más los ficheros de trabajo de análisis almacenan y tratan datos con respecto a la información económica y financiera del sujeto así como datos sobre su comportamiento, es decir sobre su estilo de vida, movimientos, lugares de frecuentación, armas y otros instrumentos peligrosos, el grado de peligrosidad del sujeto y los riesgos específicos como la probabilidad de fuga.

<sup>19</sup> En el anterior Convenio EUROPOL, esta clase de datos venían denominadas como “indicaciones personales”. El Acto del Consejo de 3 de noviembre de 1998 por el que se aprueban las normas aplicables a los ficheros de análisis de EUROPOL, art.6 que abarca como “indicaciones personales” los apellidos actuales y anteriores, nombres actuales y anteriores, apellidos de soltero/a, nombre del padre (si es necesario para proceder a la identificación), nombre de la madre (si es necesario para poder proceder a la identificación), sexo, fecha de nacimiento, lugar de nacimiento, nacionalidad, estado civil, alias, apodo, nombres utilizados o nombres falsos, residencia o domicilios actuales y anteriores”.

estatuto establecido mediante la Decisión del Consejo de 6 de abril, se prevé la posibilidad en los ficheros de trabajo de análisis, del tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas o la afiliación sindical, el tratamiento de datos relacionados con la salud o la vida sexual. Se prevé que este tratamiento se hará de manera excepcional y solamente cuando sea estrictamente necesario para la finalidad del fichero de que se trate. Se exige además que dichos datos deban completar otros datos personales introducidos en el mismo fichero<sup>20</sup>.

Hay que mencionar que el tratamiento de estos datos clasificados como especiales está expresamente prohibido por la Directiva 95/46/CE sobre protección de datos personales<sup>21</sup>. Es altamente conocido que sus disposiciones son aplicables solamente en el marco comunitario; por lo tanto, anteriormente no eran de aplicación en el llamado ámbito del Tercer Pilar de la UE. Es así que se elaboró la Decisión Marco 2008/977/JAI para cubrir el ámbito del tratamiento de los datos en el marco de la cooperación penal<sup>22</sup> y hay que subrayar que en esta Decisión se prevé la posibilidad de tratar esta categoría especial de datos cuando sea estrictamente necesario y si el Derecho nacional ofrece garantías adecuadas<sup>23</sup>.

Ahora bien, sabemos que mediante el Tratado de Lisboa se han eliminado y “comunitarizado” los antes llamados Pilares de la UE. Además, EUROPOL viene ya reconocida como una Agencia de la UE y por lo tanto a la hora de aplicar la normativa europea en materia del tratamiento de datos, podríamos encontrarnos en presencia de una “colisión” de normas: la Directiva 95/46/CE sobre protección de datos personales y la Decisión Marco 2008/977/JAI.

Como regla general, sabido es que lo que no se prohíbe explícitamente está permitido y siendo así, la posibilidad de poder tramitar estos datos sensibles entra en contradicción con la Carta de Derechos Fundamentales de la Unión Europea, la cual reconoce explícitamente en sus artículos, el derecho a la intimidad<sup>24</sup> y el derecho a la protección de datos de carácter personal<sup>25</sup> de cualquier persona. Es más, la Directiva

<sup>20</sup> Decisión EUROPOL, art. 14, punto 1. ap. 2.

<sup>21</sup> Véase al respecto la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos, DOCE L 281, de 23 de noviembre.

<sup>22</sup> Recordemos que los instrumentos de trabajo en los ámbitos intergubernamentales del antes Segundo y Tercer Pilar del TUE son las Decisiones y las Decisiones Marco.

<sup>23</sup> “El tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, de datos relativos a la salud o a la vida sexual sólo se permitirá cuando sea estrictamente necesario y si el Derecho nacional establece garantías adecuadas”. Art. 3.2, Decisión Marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, Decisión Marco 2008/977/JAI del Consejo de 27 de nov. de 2008, DOUE L 350/60, de 30.12.2008.

<sup>24</sup> Art. 7, respeto a la vida privada y familiar: “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones”.

<sup>25</sup> Art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea, especialmente dedicado a la Protección de datos de carácter personal, en donde se establece que: “(1) Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan; (2) Estos datos se tratarán de modo leal, para

95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos<sup>26</sup> abarca las normas que tratan sobre la legitimidad del tratamiento de los datos personales y sobre los derechos del interesado, incluyendo las disposiciones relativas a los recursos judiciales, responsabilidad y sanciones, pero también prevé explícitamente, tal como más arriba hemos mencionado, que sus disposiciones no se aplican a las actividades que quedan fuera del “ámbito comunitario”. Como habíamos afirmado ya, el antes denominado Tercer Pilar del TUE, el que trataba el tema de EUROPOL, quedaba fuera del ámbito comunitario, con lo cual las disposiciones de esta Directiva eran inaplicables a EUROPOL. Igual que en su anterior Convenio<sup>27</sup>, la Decisión del Consejo prevé de manera explícita que EUROPOL a la hora de ejercer sus objetivos, tendrá en cuenta los principios del Convenio N. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 1981 y la Recomendación n. R (87) 15, de 1987, por la que se regula la utilización de los datos personales en el sector policial<sup>28</sup>.

En el Sistema de Información, además de los datos especificados se pueden almacenar, tratar, modificar y utilizar ciertas “indicaciones”<sup>29</sup> con respecto a las personas que hayan sido condenadas o que sean sospechosas de haber cometido o participado en algún delito competencia de EUROPOL. Las indicaciones a las que se refiere la Decisión del Consejo, en realidad son los datos más importantes, en tanto que aportan lo necesario para realizar el perfil de un sujeto, o en el caso de los delincuentes, para realizar el perfil criminal de estos.

Para que los investigadores logren dibujar el perfil criminal de un sujeto, se necesitan datos con respecto a sus condenas anteriores<sup>30</sup> que, en caso de existir, vendrán ligados a los datos del *modus operandi*<sup>31</sup> y que estos a su vez conducen a los

---

fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación. El respecto de estas normas estará sujeto al control de una autoridad independiente”.

<sup>26</sup> Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos, DO L 281 de 23.11.1995, p.31.

<sup>27</sup> Anterior art. 14. 3, del Convenio EUROPOL.

<sup>28</sup> Capítulo V, Protección y seguridad de los datos, art. 27, Decisión del Consejo de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (EUROPOL), 2009/371/JAI.

<sup>29</sup> Art. 12. 3, Decisión del Consejo (Decisión EUROPOL): “además de los datos indicados en el apartado 2 y la mención de EUROPOL o de la unidad nacional que los haya suministrado, podrán almacenarse, modificarse y utilizarse en el sistema de información las siguientes indicaciones con respecto a las personas a que se refiere el apartado 1: delitos, hechos imputados, fecha y lugar de comisión; medios utilizados o que puedan serlo; servicios responsables del expediente y número de referencia de éste; sospecha de pertenencia a una organización delictiva; condenas, siempre que se refieran a delitos que sean competencia de EUROPOL; parte que haya introducido los datos.

<sup>30</sup> En función de los datos con respecto a sus condenas anteriores se establece el grado de peligrosidad del sujeto.

<sup>31</sup> La expresión *modus operandi* viene del latín y significa el *modo de operar*. Este término está empujado en la criminología y se usa en los casos en donde la forma de actuar es característica y reiterada. En el

datos que revelen las informaciones con respecto a los instrumentos efectivos o posibles para preparar o cometer un siguiente delito. También se almacenan los datos que revelen el grupo u organización delictiva a la que pertenece, como también la posición que tiene el sujeto en el grupo<sup>32</sup>, así como el ámbito geográfico en cual actúa que es lógicamente el ámbito en el cual se comenten las actividades delictivas.

Al tratarse de datos personales de materia policial, se exige un alto nivel de seguridad tanto para acceder a los datos así como para introducirlos en el Sistema de Tratamiento de la Información de EUROPOL. Por lo tanto, el derecho a introducir datos e implícitamente el derecho de acceso a los datos del Sistema, han quedado reservados para los funcionarios de enlace y los miembros de las Unidades Nacionales, así como para el director, los directores adjuntos y para los agentes de EUROPOL<sup>33</sup>. El acceso al sistema por parte de alguno de los mencionados será debidamente habilitado bajo una autorización en la medida en que sea necesaria para el cumplimiento de un cometido concreto y se regirá por las disposiciones legales, reglamentarias y administrativas, así como por los procedimientos de la Unidad que efectúe la consulta.

Anteriormente, el Convenio EUROPOL establecía que, para poder acceder al Sistema de Información de EUROPOL, era necesaria una previa justificación del motivo y de la necesidad de acceder a los datos, lo que llevaba tiempo y se consideraba que era un aspecto negativo para la puesta en marcha de una rápida investigación. Lógicamente, la necesidad de acceder a los ficheros se debe a la necesidad de conocer la información almacenada por motivo de su tarea o misión, y el acceso solo se autorizará a las personas que posean la debida habilitación de seguridad.

Es altamente conocido que el anterior procedimiento administrativo exigía tiempo, en tanto que era necesaria una evaluación de la solicitud de acceso, así como una evaluación compleja de la necesidad de saber y acceder a la información. El procedimiento finalizaba con una resolución en la que constaba un resultado afirmativo o negativo. Si el resultado era afirmativo, venía acompañado de un “certificado de seguridad” que permitía el acceso al Sistema y en su contenido figuraba el nombre del solicitante, la motivación de la solicitud, la información que ulteriormente era anhelada, su nivel de clasificación, así como la fecha de expiración del permiso de acceso.

Debido al largo tiempo que suponía este procedimiento y además al ser un inconveniente en lo que prevé la rápida solución de los casos pendientes, la

---

momento en que aparece el *modus operandi*, entran en *juego* las técnicas de criminalística, es decir el análisis de los esquemas intelectuales, estrategias y diversas formas utilizadas en dicho acto delictivo.

<sup>32</sup> Nos referimos a los que llevan el título de líder, participante o coadyuvante en una organización delictiva.

<sup>33</sup> El art. 13 de Decisión del Consejo de 6 de abril de 2009 por la que se crea la Oficina Europea de Policía, establece que: “El derecho a introducir directamente datos en el sistema de información de EUROPOL y de recuperarlos del mismo quedará reservado a las unidades nacionales, a los funcionarios de enlace, al director, a los directores adjuntos y a los agentes de EUROPOL debidamente habilitados. EUROPOL podrá recuperar los datos cuando sea necesario para el cumplimiento de un cometido concreto. La recuperación por parte de las unidades nacionales y los funcionarios de enlace se regirá por las disposiciones legales, reglamentarias y administrativas y procedimientos de la parte que efectúe la consulta, a no ser que la presente Decisión contenga otras disposiciones al respecto”.

consecuencia y la solución a la vez, se configuró en la Propuesta de Decisión del Consejo por la que se crea la Oficina Europea de Policía<sup>34</sup> que traía consigo una mejora, permitiendo el acceso directo a las Unidades Nacionales para consultar el Sistema de Información, considerándose que la obligación prevista en el Convenio EUROPOL que exigía la justificación de la necesidad de acceder por medio de los Funcionarios de Enlace para una investigación determinada, era demasiado incómoda para aplicarla en la práctica sin llegar a comprometer la eficacia del trabajo<sup>35</sup>.

Después de esta Propuesta que reclamaba un cambio radical de lo que era el Convenio EUROPOL, se ha llegado a la Decisión del Consejo por la que se crea la Oficina Europea de Policía<sup>36</sup> (en adelante Decisión EUROPOL) que sustituye dicho Convenio.

Pero la denominada Unidad Introdutora será la única autorizada a modificar, rectificar o suprimir los datos<sup>37</sup> que haya introducido, y la misma, al ser informada de la existencia de algunos errores que podrá contener una información en concreto, tendrá la obligación de comprobar dicha comunicación sin demora, y en caso necesario, tendrá la obligación de modificar, completar o suprimir inmediatamente la información en cuestión<sup>38</sup>. Ahora bien, si se trata de las personas que sean sospechosas de haber cometido o de haber participado en un delito que sea competencia de EUROPOL, o que hayan sido condenados por tales delitos, en este caso se prevé una excepción a la regla arriba mencionada, en tanto que cualquier Unidad tendrá la posibilidad de completar los datos, introduciendo otros datos de la misma categoría, a modo de indicaciones adicionales<sup>39</sup>.

---

<sup>34</sup> Propuesta de Decisión del Consejo por la que se crea la Oficina Europea de Policía, EUROPOL, presentada por la Comisión, COM (2006) 817 finales, que establece en su art. 11 que: "EUROPOL creará un sistema de información de EUROPOL. El sistema de información será accesible para consulta directa por parte de las unidades nacionales, los funcionarios de enlace, el director, los directores adjuntos y los agentes de EUROPOL debidamente habilitados".

<sup>35</sup> Propuesta de Decisión del Consejo por la que se crea la Oficina Europea de Policía, COM (817) final, Aspectos Jurídicos de la Propuesta y también el Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo por la que se crea la Oficina Europea de Policía EUROPOL, DOUE C 255/13 de 27.10.2007.

<sup>36</sup> Hacemos referencia a la Decisión del Consejo de 6 de abril de 2009 por la que se crea la Oficina Europea de Policía (EUROPOL), 2009/371/JAI, DOUE L 121/37 de 15.05.2009 sobre la que hemos hablado en el primer capítulo de este trabajo de investigación.

<sup>37</sup> Nos referimos a los datos relativos a las personas que sean sospechosas de acuerdo con el Derecho nacional del Estado miembro de que se trate, de haber cometido o de haber participado en un delito que sea competencia de EUROPOL, o que hayan sido condenadas por tal delito y los elementos que pueden incluir estos datos son los siguientes: 1) Apellido, apellido de soltera, nombre y en su caso, alias o nombres utilizados; 2) Fecha y lugar de nacimiento; 3) Nacionalidad; 4) Sexo; 5) Otras características útiles para su identificación, en particular rasgos físicos específicos, objetivos y permanentes.

<sup>38</sup> El art. 13 (Uso del sistema de información de EUROPOL), de la Decisión del Consejo de 6 de abril de 2009, establece que: "La parte introdutora será la única autorizada a modificar, rectificar o suprimir los datos que haya introducido. Si otra parte dispone de indicios que permitan presumir que un dato de los mencionados en el artículo 12, 2 apartado 2, contiene errores, o si desea completar tales datos, informará de ello inmediatamente a la parte introdutora. Esta deberá comprobar la comunicación sin demora y, en caso necesario, modificar, completar, rectificar o suprimir el dato inmediatamente".

<sup>39</sup> Entendemos por "indicaciones adicionales" los datos relativos a los delitos, hechos imputados, fecha y lugar de comisión; medios utilizados o que puedan serlo; servicios responsables del expediente y número de



En la Decisión EUROPOL se prevé expresamente que en el caso en que una Parte tiene la intención de suprimir<sup>40</sup> la totalidad de los datos mencionados en el art. 12, ap. 2<sup>41</sup>, introducidos por ella con respecto a una persona, y si existen datos de los mencionados en el art. 12, ap. 3<sup>42</sup>, referidos a la misma persona introducidos por otras partes, la responsabilidad en materia de protección de datos y el derecho a modificarlos, complementarlos, rectificarlos y suprimirlos con arreglo al art. 12.2, se transferirá a la otra parte que haya introducido los datos mencionados en el art. 12.3 en relación con la misma persona. Obligatoriamente, la parte que tiene la intención o incurre en el deber de suprimir los datos, deberá informar de ello a la Parte a la que corresponda la responsabilidad en materia de protección de datos. En caso de consulta de los datos almacenados en el Sistema de Información de EUROPOL, la responsabilidad de la consulta, introducción o modificación<sup>43</sup> de la información almacenada en el Sistema, recaerá en la parte que efectúa cualquiera de las actividades mencionadas y que obligatoriamente deberá ser identificable.

No obstante, como novedad, la Decisión EUROPOL deja vía libre a la posibilidad de consulta del Sistema de Información de EUROPOL también por parte de las autoridades competentes designadas a tal efecto por los Estados miembros, pero siempre y cuando la consulta se limite a averiguar únicamente si el dato solicitado se encuentra en el Sistema de Información de EUROPOL.

En lo que a la transmisión de la información existente en el Sistema de Información de EUROPOL se refiere, ésta se podrá realizar entre las Unidades Nacionales de cada Estado miembro, así como entre las Unidades Nacionales de un lado y las autoridades competentes de los Estados miembros de otro lado, en conformidad con la legislación nacional.

---

referencia de éste; sospecha de pertenencia a una organización delictiva; condenas siempre que se refieren a delitos competencia de EUROPOL.

<sup>40</sup> Los datos pueden suprimirse mediante la destrucción de su soporte, véase al respecto la Decisión Marco 2008/977/JAI 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.

<sup>41</sup> Apellido, apellido de soltera, nombre y, en su caso, alias o nombre falso utilizado; fecha y lugar de nacimiento; nacionalidad; sexo; lugar de residencia, profesión y paradero de la persona de que se trate; número de la seguridad social, permisos de conducción, documentos de identidad y datos del pasaporte; en la medida que sea necesario, otras características que pueden resultar útiles para su identificación.

<sup>42</sup> Indicaciones con respecto a las personas a que se refiere el apartado 1. Los datos introducidos se refieren a las personas que sean sospechosas de haber cometido o de haber participado en un delito que sea competencia de EUROPOL, o que hayan sido condenadas por tal delito; o datos de las personas respecto de las cuales existan indicios concretos o motivos razonables, para presumir que cometerán delitos que son competencia de EUROPOL.

<sup>43</sup> Decisión Marco 2008/977/JAI 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: "Por lo que respecta a los datos inexactos, incompletos o anticuados transmitidos a otros Estados miembros o puestos a disposición y tratados a continuación por autoridades cuasi judiciales, entendiéndose por tales las autoridades competentes para adoptar resoluciones jurídicamente vinculantes, su rectificación, supresión, o bloqueo debe efectuarse con arreglo al Derecho nacional".

### **Los ficheros de trabajo de análisis de EUROPOL**

Con respecto a los Ficheros de Trabajo, la Decisión del Consejo de 6 de abril de 2009, por la que se constituye la Oficina Europea de Policía, dispone expresamente que EUROPOL, en la medida en que sea necesario para desempeñar sus funciones, podrá almacenar, modificar y utilizar datos relativos a los delitos que sean de su competencia, incluido los delitos conexos<sup>44</sup>, en Ficheros de Trabajo de Análisis. Estos ficheros se crearán a iniciativa de EUROPOL o a petición de los Estados miembros<sup>45</sup> que hayan suministrado los datos que se referirán a las siguientes clases de sujetos: autores o sospechosos<sup>46</sup>; posibles testigos<sup>47</sup>; perjudicados o que puedan serlo<sup>48</sup> por la comisión de

<sup>44</sup> En cuanto a los delitos conexos, la Decisión del Consejo de 6 de abril de 2009, en su art. 4.3, se refiere a los delitos cometidos con objeto de procurarse los medios para perpetrar los actos para los que EUROPOL sea competente; los delitos cometidos para facilitar o consumir la ejecución de los actos para los que EUROPOL sea competente; los delitos cometidos para conseguir la impunidad de los actos para los que EUROPOL sea competente.

<sup>45</sup> Art. 13. 1, Decisión del Consejo 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 L 325/14; 11.12.2009.

<sup>46</sup> Art. 6.2, Decisión del Consejo 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: "A) Indicaciones personales: apellidos actuales y anteriores; nombres actuales y anteriores; apellidos de soltera; nombre del padre (si es necesario para proceder a la identificación); nombre de la madre (si es necesario para proceder a la identificación); sexo; fecha de nacimiento; lugar de nacimiento; nacionalidad; estado civil; alias; apodo; nombres utilizados o nombres falsos; residencia o domicilio actuales y anteriores. B) Descripción física: fisonomía; rasgos característicos (señales, cicatrices, tatuajes, etc.). C) Medios de identificación: documentos de identidad y permiso de conducción; números de documento nacional de identidad y de pasaporte si procede, números de identificación nacionales y número de la seguridad social; imágenes visuales y otras informaciones sobre el aspecto físico; información sobre identificación forense, como impresiones dactilares, perfil del ADN (establecido a partir de la parte no codificante del ADN), características de la voz, grupo sanguíneo, información dental. D) Profesión y capacitaciones: actividad laboral y profesional actual; actividad laboral y profesional anterior; título académico (escuela, universidad, profesional); aptitudes; capacitaciones y otros conocimientos (lenguas y otros). E) Información económica y financiera: datos financieros (cuentas y códigos bancarios, tarjetas de crédito, etc.); activos líquidos disponibles; acciones y otros activos; datos sobre propiedades; vínculos con sociedades y empresas; contactos bancarios y crediticios; situación fiscal; otra información que indique la forma de gestionar los asuntos financieros de una persona. F) Datos sobre el comportamiento: estilo de vida (por ejemplo, vida por encima de sus posibilidades) y costumbres; movimientos; lugares de frecuentación; armas y otros instrumentos peligrosos; peligrosidad; riesgos específicos como probabilidad de fuga, utilización de agentes dobles, conexiones con personal policial o de aduanas; aspectos y perfiles relacionados con la delincuencia; toxicomanías. G) Personas intermediarias y acompañantes, incluidos el tipo y la naturaleza del contacto o de la relación con dichas personas. H) Medios de comunicación que utiliza, como teléfono (fijo o móvil), fax, buscapersonas, correo electrónico, direcciones postales, conexiones a Internet. I) Medios de transporte que usa, por ejemplo vehículos, embarcaciones, aviones, así como información para identificar esos medios de transporte (números de matrícula). J) Datos relativos a las actividades delictivas en las que es competente EUROPOL con arreglo al artículo 4 de la Decisión EUROPOL: condenas anteriores; presunta implicación en actividades delictivas; *modus operandi*; instrumentos efectivos o posibles para preparar o cometer delitos; grupo u organización delictiva a la que pertenece y posición en el grupo u organización; función en la organización delictiva; ámbito geográfico de las actividades delictivas; material recogido durante una investigación, como imágenes fotográficas y de vídeo. K) Referencias a otras bases de datos en que haya almacenados datos sobre la persona: EUROPOL; cuerpos de policía y aduanas; otros cuerpos de seguridad; organizaciones internacionales; entidades públicas; entidades privadas. L) Información sobre personas jurídicas relacionadas con los datos a que se refieren las letras e) y j): nombre de la persona jurídica; domicilio; fecha y lugar de constitución; número de registro administrativo; forma jurídica; capital; ámbito de actividad; filiales nacionales e internacionales; directivos; relaciones con bancos".

hechos delictivos; personas intermediarias y acompañantes<sup>49</sup>, personas que sean consideradas posibles testigos<sup>50</sup>, así como personas que pueden facilitar información<sup>51</sup>

---

<sup>47</sup> Art. 6. 5, Decisión del Consejo 2009/936/JAI, de 30 de noviembre de 2009, por la que se adoptan normas de desarrollo aplicables a los ficheros de trabajo de análisis de EUROPOL: “Con respecto a las personas que, como indica el artículo 14, apartado 1, letra b), de la Decisión EUROPOL, sean consideradas posibles testigos en investigaciones sobre los delitos considerados o en una futura causa penal, se podrán almacenar datos mencionados en el apartado 2, letra a), punto 1, a letra c), punto 3, así como las siguientes categorías de datos: a) información relacionada con delitos proporcionada por tales personas, incluida la información sobre sus relaciones con otras personas incluidas en el fichero de trabajo de análisis; b) si debe garantizarse su anonimato; c) si debe garantizarse su protección y por quién; d) nueva identidad; e) si es posible su comparecencia ante los tribunales”.

<sup>48</sup> Art. 6. 4, Decisión del Consejo 2009/936/JAI, de 30 de noviembre de 2009, por la que se adoptan normas de desarrollo aplicables a los ficheros de trabajo de análisis de EUROPOL: “Con respecto a las personas que, como indica el artículo 14, apartado 1, letra c), de la Decisión EUROPOL, hayan sido perjudicadas por uno de los delitos considerados o respecto de las cuales existan motivos para presumir que puedan verse perjudicadas por tal delito, se podrán almacenar datos mencionados en el apartado 2, letra a), punto 1, a letra c), punto 3, del presente artículo, así como las siguientes categorías de datos: a) datos de identificación de la víctima; b) motivos por los que ha sufrido el delito; c) daños sufridos (físicos, financieros, psicológicos u otros); d) si debe garantizarse su anonimato; e) si es posible su comparecencia ante los tribunales; f) información relacionada con delitos proporcionada por las personas a que se refiere el artículo 14, apartado 1, letra c), de la Decisión EUROPOL, o a través de ellas, incluida la información sobre sus relaciones con otras personas, si fuera necesario para identificar a las personas mencionadas en el artículo 12, apartado 1, de la Decisión EUROPOL”.

<sup>49</sup> Se considerará “personas intermediarias y acompañantes”, a aquellas personas respecto a las cuales existan motivos suficientes para creer que a través de ellas puede obtenerse información que se refiera a los autores o sospechosos de haber cometido delitos competencia de EUROPOL y que sea de interés para el análisis. Se considerarán “personas intermediarias” aquellas que tengan contactos esporádicos con las personas mencionadas y se considerarán “acompañantes” aquellas personas que tengan contactos periódicos con los autores o sospechosos de haber cometido delitos competencia de EUROPOL. Con respecto a las personas intermediarias y acompañantes, los datos podrán almacenarse si fuera preciso, siempre que haya motivos para presumir que tales datos son necesarios para el análisis de la función de dichas personas como personas intermediarias o acompañantes. En este contexto se observará lo siguiente: a) la relación de dichas personas con las personas a que se refiere el artículo 14, apartado 1, letra a), de la Decisión EUROPOL se aclarará lo antes posible; b) los datos se eliminarán inmediatamente si resulta infundada la presunción de que existe una relación entre dichas personas y las personas a que se refiere el artículo 14, apartado 1, letra a), de la Decisión EUROPOL; c) todos los datos contemplados en el apartado 2 podrán almacenarse si dichas personas son sospechosas de haber cometido un delito respecto del cual EUROPOL sea competente en virtud del artículo 4 de la Decisión EUROPOL, o han sido declaradas culpables de dicho delito o, según la legislación nacional del Estado miembro en cuestión, existen indicios concretos o motivos razonables para creer que van a cometer tal delito; d) no deberán almacenarse datos sobre personas intermediarias y acompañantes de personas intermediarias, ni datos sobre personas intermediarias y acompañantes de acompañantes, excepto aquellos datos sobre el tipo y naturaleza de sus contactos o relaciones con las personas a que se refiere el apartado 2; e) si no se puede llegar a determinar los aspectos indicados en las letras precedentes, se tendrá esto en cuenta para decidir sobre la necesidad y el alcance del almacenamiento para el posterior análisis” (art. 6. 3, Decisión del Consejo 2009/936/JAI, de 30 de noviembre de 2009, por la que se adoptan normas de desarrollo aplicables a los ficheros de trabajo de análisis de EUROPOL).

<sup>50</sup> De conformidad con la ley nacional de cada Estado miembro del que se trate en un caso concreto, los testigos, en función del grado de riesgo o peligro que corre su seguridad o la seguridad de su cónyuge, o persona a quien se halle ligado por análoga relación de afectividad o sus ascendientes, descendientes o hermanos, también gozarán de protección jurídica (Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales, legislación española). En cuanto a los datos que se pueden almacenar al respecto en los ficheros de análisis de EUROPOL, éstos se refieren a las siguientes categorías: a) información relacionada con delitos proporcionada por tales personas, incluida la información sobre sus relaciones con otras personas incluidas en el fichero de trabajo de análisis; b) si debe garantizarse su anonimato; c) si debe garantizarse su protección y por quién; d) nueva identidad; e) si es posible su comparecencia ante los tribunales, art. 6. 5, Decisión del Consejo 2009/936/JAI, de 30 de noviembre de 2009,



sobre los delitos que son competencia de la Oficina Europea de Policía<sup>52</sup>. Anteriormente, el Convenio EUROPOL, a la hora de hablar sobre los Ficheros de Trabajo de Análisis los presentaba como “otros ficheros”, aunque quizá debiese haber usado desde el principio la denominación que les ofrecía en los siguientes artículos, evitando de esta forma la confusión que había ocurrido al respecto. El fallo de redacción daba lugar a interpretación de que el SIE abarcaba dos clases de ficheros, es decir: los que se suponía que existían (que quizá se podrían haber denominado Ficheros X), y los Ficheros de Trabajo con Fines de Análisis que se hubiesen podido abrir en la medida en que hubiese resultado necesaria su existencia, tal como preveía explícitamente el anterior Convenio EUROPOL.

Ahora bien, la Decisión EUROPOL mejora la redacción con respecto a los Ficheros de Trabajo de Análisis, y, más todavía, los datos que antes se suponía que estos ficheros podrían almacenar, ahora se prevé de manera expresa su posibilidad de tratamiento<sup>53</sup>.

Los denominados Ficheros de Trabajo con fines de análisis<sup>54</sup> entran así en la llamada categoría de ficheros automatizados de datos personales<sup>55</sup> para los que se necesita una disposición de creación, que requerirá el acuerdo del Consejo de Administración<sup>56</sup> y abarcará elementos de identificación, denominación, objetivo, categorías de personas acerca de las cuales se vayan almacenando datos, la

---

por la que se adoptan normas de desarrollo aplicables a los ficheros de trabajo de análisis de EUROPOL.

<sup>51</sup> En este caso, se podrán almacenar las siguientes categorías de datos: apellidos actuales y anteriores; números de identificación nacionales y número de la seguridad social; indicaciones personales codificadas; tipo de información suministrada; si debe garantizarse su anonimato; si debe garantizarse su protección y por quién; nueva identidad; si es posible su comparecencia ante los tribunales; experiencias negativas; recompensas (económicas o en servicios), art. 6. 6, Decisión del Consejo 2009/936/JAI, de 30 de noviembre de 2009, por la que se adoptan normas de desarrollo aplicables a los ficheros de trabajo de análisis de EUROPOL.

<sup>52</sup> Las competencias de EUROPOL abarcarán la delincuencia organizada, el terrorismo y otras formas de delitos graves que figuran en el Anexo de la Decisión del Consejo de 6 de abril de 2009, en la medida en que dos o más Estados miembros se vean afectados de tal modo que, debido al alcance, gravedad y consecuencias de los actos delictivos, se requiera una actuación común de los Estados miembros (art. 4.1, Decisión del Consejo de 6 de abril de 2009).

<sup>53</sup> Entendemos por “tratamiento de datos personales” o “tratamiento”: “cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, 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”; Decisión del Consejo 2009/936/JAI, de 30 de noviembre de 2009, por la que se adoptan normas de desarrollo aplicables a los ficheros de trabajo de análisis de EUROPOL.

<sup>54</sup> Según el art. 14. 2, Decisión del Consejo de 6 de abril de 2009: “Los ficheros de trabajo de análisis se crearán con fines de análisis, entendiendo por análisis el ordenamiento, tratamiento o utilización de datos para facilitar investigaciones penales”.

<sup>55</sup> Dentro de los ficheros automatizados de datos personales se pueden crear los denominados ficheros temporales, que deberán cumplir con las normas impuestas al respecto para la seguridad de los datos personales que se están almacenado. Estos datos serán borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación. Los datos dejarán de ser necesarios cuando, por ejemplo: la investigación del caso que es la base de la creación de dicho fichero temporal haya finalizado, o en caso de que los datos almacenados que se suponía que corresponden a un sospechoso de haber cometido el delito que se investiga, al final se comprueba que la persona no es culpable.

<sup>56</sup> Según el art. 37.1 de la Decisión del Consejo de 6 de abril de 2009, el Consejo de Administración estará compuesto por un representante de cada Estado miembro y un representante de la Comisión.

proveniencia de los datos que se vayan a almacenar, tipos de datos personales que permiten el acceso total al fichero, transferencia o introducción de los datos, las condiciones en que podrán transmitirse los datos de dicho fichero, a qué destinatarios y bajo qué procedimiento, los plazos de verificación y la duración del almacenamiento, así como la constancia documental<sup>57</sup>.

La Decisión de EUROPOL prevé la posibilidad, cuando sea estrictamente necesario para la finalidad del fichero de que se trate, que se realice el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas o la afiliación sindical y el tratamiento de datos relacionados con la salud o la vida sexual. Imprescindiblemente, esta categoría de datos sensibles serán tratados única y exclusivamente para completar otros datos personales almacenados y tratados en el mismo fichero, con la prohibición de seleccionar una categoría particular de personas a partir únicamente de los datos sensibles mencionados<sup>58</sup>.

En su labor, tanto EUROPOL como las Unidades Introdutoras (de datos) deberán respetar la legislación en materia de protección de datos en el ámbito policial. Por lo tanto, conviene recordar que los datos sensibles arriba mencionados no podrán tratarse automáticamente, a menos que el derecho interno prevea garantías apropiadas, y la misma norma regirá en el caso de datos de carácter personal referentes a condenas penales<sup>59</sup>.

Anteriormente, el Convenio EUROPOL, al hacer referencia a estos datos especiales, los catalogaba como “información adicional”<sup>60</sup> a pesar de que entran en el llamado ámbito de la vida privada, en tanto que la vida privada se puede ver afectada tanto a través de la vigilancia efectuada y de la recopilación secreta de información personal de los sujetos en cuestión por parte de las autoridades públicas, así como, si se da el caso, por la divulgación a terceros de información confidencial obtenida por los poderes públicos en el marco de sus funciones públicas (Lasagabaster Herrarte, 2004: 288).

Hay que subrayar que, a pesar de que el Convenio ha sido sustituido por la Decisión EUROPOL, se ha optado por la misma redacción al respecto, catalogando los datos especiales como información adicional.

Los Ficheros de Trabajo con Fines de Análisis podrán ser de naturaleza<sup>61</sup> general

---

<sup>57</sup> Decisión del Consejo de 6 de abril de 2009, art. 16, “Orden de creación de un fichero de trabajo de análisis”.

<sup>58</sup> Art. 14, punto 1, ap. 2, Decisión EUROPOL.

<sup>59</sup> Art. 6 del 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.

<sup>60</sup> Anterior Convenio EUROPOL, art. 10: “(...) y cuando tales datos completen otros datos personales introducidos en el mismo fichero”.

<sup>61</sup> La elaboración de análisis operativos supone el intento de ver allí donde los investigadores no pueden ver por la amplia cantidad de información, iniciando así nuevas líneas de investigación a raíz de hallazgos en la información. En cuanto a los llamados análisis estratégicos, en tanto que descripción de la situación actual, nos referimos aquí al informe de situación, caracterizado como puramente descriptivo. Del mismo modo se

o estratégica, cuando el objetivo sea tratar información pertinente sobre un problema particular, o desarrollar o mejorar las iniciativas de las autoridades competentes de los Estados miembros, así como de naturaleza operativa, cuando el fin sea recabar información relativa a un caso, persona u organización sobre alguna de las actividades delictivas competencia de EUROPOL, para investigaciones bilaterales o multilaterales de alcance internacional, siempre que las partes interesadas sean dos o más Estados miembros.

Las conclusiones de los análisis de EUROPOL llevan forma de informes de evaluación de la amenaza, en donde se establecen una serie de parámetros estudiándose la motivación y la capacidad como factores básicos que definen la amenaza en concreto. Las dos clases de análisis estratégicos de las cuales se encarga habitualmente EUROPOL son el informe de situación y tendencias, que se hace anualmente de octubre a octubre, y el informe evaluación de la amenaza, que se hace cada vez que se considera oportuno. Los dos trabajos de análisis se basan en información que los cuerpos especializados de los Estados miembros remiten a EUROPOL<sup>62</sup>.

Las Unidades Nacionales de los Estados miembros<sup>63</sup>, por iniciativa propia o a solicitud de EUROPOL, comunicarán a la Agencia toda la información que ésta necesite a efectos del Fichero de Trabajo de Análisis. En caso de que el análisis que se elabora es de tipo general o estratégico, se mantendrán plenamente asociados a todos los Estados miembros. Per a contrario, si la labor de análisis se refiere a casos particulares que no afecten a todos los Estados miembros y tiene una orientación operativa directa, estarán autorizados a participar en ello solamente aquellos Estados de donde proviene la información por la que se haya abierto el fichero, o aquellos Estados que se ven afectados, así como aquellos que el grupo de análisis invite posteriormente a asociarse al haberse convertido en partes afectadas.

También podrán obtener la autorización de acceso al fichero de análisis de un caso concreto, aquellos que tras consultar el Sistema de Índice se hallan en la necesidad

---

encarga de lo que se llama análisis de tendencia, que a veces se mezclan con los informes de situación, produciendo informes de situación y tendencias con el objetivo de establecer y analizar la tendencia que se sigue en el ámbito delictivo (Carrera Hernández, 2003: 104).

<sup>62</sup> Véase [https://www.europol.europa.eu/latest\\_publications/25](https://www.europol.europa.eu/latest_publications/25)

<sup>63</sup> Los datos personales transmitidos o puestos a disposición por la autoridad competente de otro Estado miembro únicamente podrán tratarse posteriormente (...), para los siguientes fines distintos de aquellos para los que se transmitieron o se pusieron a disposición: 1) La prevención, investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales distintas de aquellas para las que se transmitieron o se pusieron a disposición; 2) Otros procedimientos judiciales y administrativos, directamente relacionados con la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales; 3) La prevención de amenazas inmediatas y graves a la seguridad pública; 4) Cualquier otro fin, solo con el previo consentimiento del Estado miembro transmisor o con el consentimiento del interesado, otorgados de acuerdo con el derecho nacional. Véase al respecto la Decisión marco 2008/977/JAI del Consejo de 27 de noviembre de 2008, relativo a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. DOUE L 350/60 de 30.12.2008.

de conocer la información que almacena y trata dicho fichero<sup>64</sup>. Por lo tanto, subrayamos que los datos que se almacenan en los ficheros del Sistema de Información de EUROPOL se aportan por los Estados miembros o por los agentes de EUROPOL, o son el resultado del tratamiento de los datos personales (Arenas Ramiro, 2006: 299)<sup>65</sup>, y éstos estarán introducidos en el Sistema siempre y cuando afecten a dos o más Estados miembros.

El Estado que aporta los datos al Sistema de Información de EUROPOL<sup>66</sup> (denominado Estado transmisor), es el que los transfiere<sup>67</sup> al Estado afectado (denominado Estado interesado) y a la hora de hacer la transferencia de datos personales, tendrá en cuenta las normas y las garantías que se imponen al respecto por su legislación nacional. Hay que subrayar que cada transmisión de datos de carácter personal contenidos en los ficheros de análisis quedará registrada en el mismo y antes de efectuar la transmisión, EUROPOL junto con el Estado transmisor, verificará la exactitud y la conformidad de los datos con lo establecido en la Decisión EUROPOL<sup>68</sup>.

La Decisión EUROPOL prevé que el Estado miembro destinatario deberá informar al Estado miembro transmisor de la utilización que se haya hecho de los datos recibidos, así como de los resultados obtenidos. Eso sí, siempre y cuando la legislación del Estado miembro destinatario permita el informe de estos aspectos<sup>69</sup>.

El ámbito de la materia de protección de datos personales en materia de cooperación policial, si que siendo débil a causa de la inexistencia de textos internacionales, remitiéndonos solo a las escasas normas previstas en los acuerdos ratificados por los Estados. Todo esto tiene como consecuencia una mayor incertidumbre a la hora de hablar sobre las transferencias internacionales de datos, más aún cuando “la especial volatilidad de las transferencias de datos complica extraordinariamente la definición del derecho sustantivo aplicable, en lo que algunos autores han calificado

---

<sup>64</sup> Art. 14, p. 3 y 4, Decisión del Consejo de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía, 2009/371/JAI, DOUE L 121/37, 15.5.2009.

<sup>65</sup> Afirma el autor: “Un tratamiento de datos personales es cualquier operación o conjunto de operaciones realizada con datos personales, independientemente de si se lleva a cabo por procedimiento automatizado o manual, siempre que los datos estén almacenados o estarán almacenados en los ficheros”.

<sup>66</sup> Anteriormente, en el Convenio EUROPOL, art. 15, p.3, se especificaba que EUROPOL almacenaba los datos de manera que se pudiese determinar por qué Estado miembro o Estado u organismo tercero habían sido transmitidos o si eran el resultado de análisis realizados por EUROPOL.

<sup>67</sup> Con respecto a la transferencia de los datos y a las condiciones que debe cumplir la transferencia internacional de datos personales, nos remitiremos a las disposiciones del Convenio 108 y de su Protocolo Adicional. En su Preámbulo reconoce la importancia de los flujos transfronterizos de información entre los pueblos (entendemos por “pueblos” los Países Signatarios del C108 y del Protocolo Adicional), considerando al mismo tiempo que “con el incremento del intercambio de datos personales a través de las fronteras, es necesario asegurar la afectiva protección de los Derechos humanos y libertades fundamentales y, en especial, el derecho a la privacidad, en relación con tales intercambios”. Véase el Preámbulo del Protocolo Adicional del C108 para la protección de las personas con respecto al tratamiento automatizado de carácter personal y relativo a transferencia de datos.

<sup>68</sup> Art. 15.1, Decisión del Consejo 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.

<sup>69</sup> Art. 15.1, Decisión del Consejo 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.

acertadamente como desterritorialización cualificada. Las características de los flujos de información y el carácter abierto de las redes hacen que los datos puedan ser accedidos, recopilados y tratados desde varios países de manera simultánea, por lo que distintos Estados tendrán competencia normativa para definir los términos y las condiciones de las prácticas apropiadas en el ámbito de la información” (García Beato, 2002: 198).

Se ha optado por el C108 como el conjunto de normas al que se le reconoce el objetivo de poner orden en el asunto de los flujos transfronterizos de datos de carácter personal en relación con el derecho interno<sup>70</sup>, enunciándose de esta forma una regla general que ha de imperar entre los Estados miembros del Consejo de Europa que han ratificado el instrumento internacional aludido, esto es, el principio de libre circulación de datos entre los Estados partes (Pavón Pérez, 2001-2002: 249)

Con carácter general, cabe destacar el particular rigor con el que se establece la exigencia de adecuación del uso a la finalidad<sup>71</sup> prevista, así como la calidad<sup>72</sup> de los datos que se transfieren y la licitud del tratamiento y de la transferencia en sí. El Estado transmisor le puede restringir al Estado interesado los posibles usos a que destine los datos personales transferidos, y fijar de esta forma las condiciones para el debido uso de los datos transmitidos (Martínez Martínez, 2001: 290).

Es imprescindible que a la hora de efectuar una transmisión de datos de carácter personal a otro Estado miembro o tercero, dentro del Sistema de Información de EUROPOL exista un Fichero de Datos o un Registro que abarque toda la información con respecto a las transferencias de datos realizadas: datos de identificación del Estado transmisor y del Estado receptor; la información transmitida y su nivel de seguridad; las garantías ofrecidas para la protección de estos datos en el derecho nacional del Estado transmisor y en el Derecho nacional del Estado receptor; los fines para los que se hace la transferencia de estos datos; las restricciones si es el caso de los posibles usos de la información.

<sup>70</sup> Véase al respecto el C108, cap. III, art. 12.

<sup>71</sup> Los datos deben ser recogidos, almacenados y tratados para unos fines determinados y legítimos y no deben ser utilizados de manera incompatible con tales fines. Lo mismo pasa en el caso de transferencia de estos datos, no pueden ser utilizados más que por el fin que ha sido base de la solicitud de transmisión. La posibilidad de cambio de los fines esta prevista en art. 6 del Reglamento (CE) N. 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (aplicable solo al ámbito comunitario): “1) Los datos personales sólo podrán tratarse con fines distintos de los que motivaron su recogida cuando este cambio de fin esté permitido expresamente por normas internas de la institución o del organismo comunitario; 2) Los datos personales recogidos exclusivamente para garantizar la seguridad o el control de los sistemas o las operaciones de tratamiento no se utilizarán con ningún otro fin, salvo los de la prevención, la investigación, la detección y la represión de infracciones penales graves”.

<sup>72</sup> Con respecto a la calidad de los datos personales que se transmitirán, recordemos que “los datos de carácter personal que sean objeto de un tratamiento automatizado: a) se obtendrán y tratarán leal y legítimamente; b) se registrarán para finalidades determinadas y legítimas, y no se utilizaran de una forma incompatible con dichas finalidades; c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; d) serán exactos y si fuera necesario puestos al día; e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un periodo de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado”.



Hay que poner de relieve que el principio de libre circulación de datos en materia de cooperación policial en materia penal se ve limitado en la medida en que la legislación de un Estado parte prevé una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal<sup>73</sup>, por razón de naturaleza de dichos datos o ficheros, o cuando la transmisión de los datos personales se lleve a cabo a partir de su territorio hacia el territorio de otra parte, con el fin de evitar que dichas transmisiones tengan como resultado evitar cumplir con la legislación del otro Estado<sup>74</sup>.

El Protocolo Adicional<sup>75</sup> del C108 se refiere específicamente a los flujos transfronterizos de datos personales hacia un destinatario que no esté sometido a la jurisdicción de un Estado parte en el Convenio, y en su Informe Explicativo pone de relieve que la regla general en este caso es que la transferencia de datos internacionales se hará sólo a aquellos Estados u Organizaciones internacionales que aseguran un nivel de protección adecuado que será evaluado tomando en cuenta todas las circunstancias del caso. Las autoridades de cada Estado parte, de conformidad con su derecho interno, se harán cargo de vigilar el cumplimiento de este aspecto<sup>76</sup>. Las excepciones<sup>77</sup> de la regla

---

<sup>73</sup> Quizás se debería tener en cuenta los datos clasificados por los cuatro niveles de seguridad en función del grado de secreto que se le confiere. Sabido es que los niveles de clasificación de EUROPOL son: *EUROPOL Restricted*, *EUROPOL Confidential*, *EUROPOL Secret* y *EUROPOL Top Secret*. Cada uno de los niveles de clasificación de EUROPOL remitirá a una batería de seguridad específica, que deberá aplicarse en EUROPOL. Las baterías de seguridad ofrecerán distintos niveles de protección, de acuerdo con el contenido de la información y teniendo en cuenta los efectos perjudiciales que el acceso, la difusión o la utilización no autorizados de la información pudieran tener para los intereses de EUROPOL o de los Estados miembros. Véase al respecto el Acto del Consejo de 5 de junio de 2003 que modifica el Acto del Consejo de 3 de noviembre de 1998 por el que se adoptan normas sobre protección del secreto aplicables a la información de EUROPOL, 2003/C 152/01.

<sup>74</sup> Art. 12, ap. 3 del Convenio 108.

<sup>75</sup> Este Protocolo que trata explícitamente el tema relativo a la transferencia de datos, a fecha de 9 de enero de 2002, ha sido firmado por sólo 15 Estados miembros del Consejo de Europa (los Estados firmantes son: Austria, Dinamarca, Finlandia, Francia, Alemania, Grecia, Islandia, Italia, Lituania, Noruega, Portugal, Eslovaquia, Suecia, Turquía, Reino Unido. Un Estado Signatario del Protocolo no podrá ratificarlo, aceptarlo o aprobarlo sin haber ratificado, aceptado o aprobado con carácter previo o de manera simultánea, el Convenio o sin haberse adherido a dicho Convenio 108.) y ratificado solo por un Estado (Suecia). En los primeros dos artículos se abordan las cuestiones con respecto al nombramiento de autoridades de control y al flujo internacional de datos personales para que después se prevén explícitamente las reglas y las excepciones con respecto a la transferencia de datos, tanto entre los Estados parte en el Convenio así como entre un Estado parte en el Convenio y un Estado u Organización internacional que no lo sea. Según Juan Antonio Pavón: "El Informe Explicativo del Protocolo apunta a que la multiplicación de los flujos internacionales de datos personales tiene su origen más inmediato, como no es muy difícil de adivinar, en la globalización de los intercambios internacionales y en la rápida evolución de las muy diversas aplicaciones de los progresos experimentados en el campo de las nuevas tecnologías, lo que a su vez requiere, de manera paralela, una mejora constante de la protección efectiva de los derechos garantizados por el Convenio en el contexto más amplio de los Derechos humanos del individuo. Así la búsqueda de la efectividad de esta protección implica una armonización internacional, no solo de los principios fundamentales de la protección datos, sino también, en cierta medida, de los medios de poner en marcha estos principios y de las condiciones en las que han de efectuarse las transferencias internacionales de datos a través de las fronteras" (Pavón, 2001 -2002: 242).

<sup>76</sup> Entendemos que la norma se refiere a cada Estado parte emisor de los datos que van a ser transferidos al Estado que no hace parte del C108.

<sup>77</sup> El art. 2.2 del Protocolo Adicional del C108 que trata sobre la Transferencia de datos personales a destinatarios no sometidos a la competencia de las Partes del Convenio, establece que "no será de aplicación

general autorizan la transferencia de datos personales en dos supuestos: 1) cuando el derecho interno así lo establece a causa de intereses concretos del afectado, o cuando se trata de intereses legítimos especialmente de los de carácter público; 2) cuando las garantías resultan de las “cláusulas contractuales, por parte del responsable del tratamiento, responsable de la transferencia y dichas garantías se estiman adecuadas por las autoridades competentes de conformidad con el derecho interno”.

### **Función de Índice**

El tercer elemento del Sistema de Información de EUROPOL es la Función de Índice<sup>78</sup> de los datos almacenados en los Ficheros de Trabajo con Fines de Análisis. En la Decisión EUROPOL se prevé expresamente que el director, los directores adjuntos, el personal de EUROPOL, los funcionarios de enlace y los miembros de las Unidades nacionales, debidamente habilitados, tendrán reconocido el derecho a consultar la Función de Índice. El acceso estará muy limitado, en tanto que permitirá solamente determinar si una información está o no almacenada en un fichero de análisis.<sup>79</sup>

La Función de Índice estará constituida de tal manera que indique claramente a la persona que la utilice si un fichero de trabajo de análisis contiene información que resulte de utilidad e interés para la realización de la investigación o tareas que le incumben al consultante<sup>80</sup>.

Es importante subrayar que la Función de Índice no se constituye como parte de la base de datos recopilados, almacenados, analizados y tratados por EUROPOL, sino que es más bien un detalle agregado al Sistema de Tratamiento de la Información de EUROPOL.

## **INFORMACIÓN CLASIFICADA**

El papel de la información en la lucha contra la criminalidad organizada es incuestionable y en lo que respecta a los ficheros constituidos para llevar a cabo investigaciones concretas es importante señalar que sus características especiales determinan su regulación en tanto al tratamiento<sup>81</sup> que requieren. Ahora bien, en función

---

el párrafo 1 del artículo 2 del presente Protocolo, pudiendo las Partes autorizar la transferencia de datos personales: a) si el derecho interno así lo establece a causa de intereses concretos del afectado, o intereses legítimos, especialmente los de carácter público; b) si se prevén las suficientes garantías, que pueden resultar, en particular, de cláusulas contractuales, por parte del responsable del tratamiento, responsable de la transferencia y dichas garantías se estiman adecuadas por las autoridades competentes de conformidad con el derecho nacional”.

<sup>78</sup> En el anterior Convenio EUROPOL, la Función de Índice era denominada como Sistema de Índice.

<sup>79</sup> Art. 15, Decisión del Consejo de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía, EUROPOL, 2009/371/JAI.

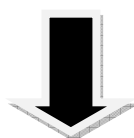
<sup>80</sup> Art. 15, Decisión del Consejo de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía, EUROPOL, 2009/371/JAI.

<sup>81</sup> Se entiende por “tratamiento de datos personales” o “tratamiento”: “cualquier operación o conjunto de operaciones efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales o no personales, como la recogida, registro, organización, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso,

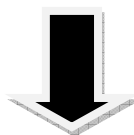
de las características de los ficheros automatizados de datos tratados por EUROPOL, consideramos que se podrán dividir en cuatro grandes categorías a las que se les asigna el nivel y las medidas de seguridad teniendo en cuenta la clase de información<sup>82</sup> que almacenan.

### Esquema jerárquico

#### 3. NIVEL CLASIFICACIÓN



#### 2. LAS CLASES DE DATOS



#### 1. FICHERO AUTOMATIZADO DE DATOS

Los niveles de clasificación<sup>83</sup> de los datos tratados por EUROPOL se dividen en cuatro categorías, es decir: 1) *EUROPOL RESTRICTED*-EUROPOL Difusión Limitada; 2) *EUROPOL CONFIDENTIAL*-EUROPOL Confidencial; 3) *EUROPOL SECRET*-EUROPOL Reservado; 4) *EUROPOL TOP SECRET*-EUROPOL Secreto.

Toda la información tratada por EUROPOL o a través de EUROPOL dentro de su organización se someterá a las altas medidas de seguridad establecidas para cada nivel de clasificación y cada Estado miembro se comprometerá a garantizar que la información de EUROPOL recibirá, en su territorio, un nivel de protección equivalente al nivel de protección ofrecido en la Decisión por la que se adoptan las normas de confidencialidad de la información de EUROPOL<sup>84</sup>, así como en conformidad con su manual interno de

---

cotejo o interconexión, así como su bloqueo, eliminación o destrucción". Véase la Decisión del Consejo 2009/936/JAI, de 30 de noviembre de 2009, por al que se adoptan las normas de desarrollo aplicables a los ficheros de trabajo de índice.

<sup>82</sup>Asociamos la "clase de información" con la "información clasificada", que según la Decisión 2009/968/JAI se considera toda información o material de cualquier forma cuya divulgación no autorizada pueda causar varios grados de perjuicio a los intereses esenciales de EUROPOL o de uno o varios Estados miembros.

<sup>83</sup> Según 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, el nivel de clasificación se define como un marcado de seguridad atribuido a los documentos tratados por EUROPOL o a través de EUROPOL.

<sup>84</sup> Decisión 2009/968/JAI del Consejo, de 30 de noviembre, DOUE L 332/17, 17.12.2009.



seguridad<sup>85</sup>. Para una estrecha colaboración entre EUROPOL y las Unidades Nacionales de los Estados miembros, se utilizan los canales de comunicación<sup>86</sup> que las mismas deberán tener un nivel de protección adecuado para cada una de las clases de datos que se transfieren mediante esta vía de conexión. Para garantizar la seguridad de las conexiones electrónicas, es el Comité de Seguridad<sup>87</sup> el que previa consulta a los servicios competentes de los Estados miembros aprobará por unanimidad una norma común.

Hemos visto a lo largo de este trabajo que la Decisión EUROPOL establece que los datos personales almacenados y tratados con fines de análisis se dividen en cinco grandes categorías<sup>88</sup>. La primera categoría abarca los datos relacionados con los condenados por haber cometido algún delito que cae bajo competencia de la Agencia y los sospechosos de que hayan cometido o que van a cometer tales delitos. La segunda categoría comprende los datos personales relativos a las víctimas que hayan sido perjudicadas por uno de los delitos competencia de EUROPOL y las presuntas víctimas con respecto a cuales existen motivos, o indicios para considerar que puedan ser perjudicadas por tales delitos. En la tercera categoría están incluidos los datos relativos a los posibles testigos en un caso de delincuencia organizada. La cuarta categoría contiene los datos relativos a las personas intermediarias y acompañantes. Y la quinta categoría almacena datos con respecto a las personas que puedan facilitar información sobre los delitos considerados.

Ahora bien, en cuanto a los niveles de clasificación de EUROPOL y a los datos personales que trata, el primer nivel es el de difusión restringida-*EUROPOL Restricted*, en tanto que abarca sólo la “información y el material cuya revelación<sup>89</sup> no autorizada

---

<sup>85</sup> El Manual de Seguridad de EUROPOL se aprobará por parte del Consejo de Administración previa consulta al Comité de Seguridad y proporcionará orientaciones de gestión y apoyo a la seguridad de conformidad con las necesidades operativas y establecerá el planteamiento de EUROPOL de la gestión de seguridad. Se prevé que incluirá normas de desarrollo de las medidas de seguridad que deberán aplicarse en EUROPOL y que proporcionen el nivel básico de seguridad, así como normas de desarrollo de las medidas de seguridad relacionadas con los distintos niveles de clasificación de EUROPOL y las correspondientes a las baterías de seguridad. Las baterías de seguridad se definen como una combinación específica de medidas de seguridad que se aplicarán a la información en función del nivel de clasificación de EUROPOL; véase el art. 7 de la Decisión 2009/968/JAI del Consejo, de 30 de noviembre, DOUE L 332/17, 17.12.2009, por la que se adoptan las normas sobre confidencialidad de la información de EUROPOL.

<sup>86</sup> Art. 2.2, Decisión 2009/968/JAI del Consejo, de 30 de noviembre, DOUE L 332/17, 17.12.2009, por la que se adoptan las normas sobre confidencialidad de la información de EUROPOL.

<sup>87</sup> El Comité de Seguridad está integrado por representantes de los Estados miembros y de EUROPOL y tendrá como misión asesorar al Consejo de Administración y al director de EUROPOL respecto a las normas de seguridad, así como a la aplicación del manual de seguridad. El Comité de Seguridad de EUROPOL tendrá un reglamento interno y se establecerá un Coordinador de Seguridad que asumirá la responsabilidad general de todas las cuestiones relativas a la seguridad, y será directamente responsable ante el director de EUROPOL; véase los art. 4 y 5 de la Decisión 2009/968/JAI del Consejo, de 30 de noviembre, DOUE L 332/17, 17.12.2009, por la que se adoptan las normas sobre confidencialidad de la información de EUROPOL.

<sup>88</sup> Art. 14.1 Decisión del Consejo de 6 de abril de 2009 por la que se crea la Oficina Europea de Policía EUROPOL, 2009/371/JAI.

<sup>89</sup> Es importante subrayar que antes de la reforma de 2009 del *estatuto* de EUROPOL, en el Acto que preveía los niveles de clasificación y protección de los datos de su sistema se hablaba de la “difusión de la

podrá resultar desfavorable para los intereses esenciales de EUROPOL, de la UE, o de uno o varios Estados miembros”. Al no tener conocimiento expreso de la categoría de datos a la que hacen referencia las normas<sup>90</sup>, podríamos considerar este primer nivel como el *nivel básico*<sup>91</sup> de la clasificación y que los ficheros clasificados como *EUROPOL Restricted* almacenan datos de carácter personal que se refieren a las personas que sean sospechosas de haber cometido o de haber participado en un delito de su competencia, así como las personas que han sido condenadas por tal delito.

La Decisión EUROPOL establece que en la medida en que sea necesario para desempeñar sus funciones, la Agencia podrá almacenar, modificar y utilizar datos personales pertenecientes a las personas “que sean consideradas posibles testigos en investigaciones sobre los delitos considerados o en una futura causa penal; personas que hayan sido perjudicadas por uno de los delitos considerados o con respecto de los cuales existen motivos para presumir que puedan ser perjudicadas por tal delito; personas intermediarias y acompañantes, así como las personas que puedan facilitar información sobre los delitos considerados”<sup>92</sup>. Analizando este aspecto, consideramos que los datos personales que vamos a clasificar como *EUROPOL Restricted*-nivel básico se refieren a la primera y cuarta categoría de personas y abarca indicaciones personales: apellidos actuales y anteriores; nombres actuales y anteriores; apellidos de soltera; nombre del padre (si es necesario para proceder a la identificación); nombre de la madre (si es necesario para proceder a la identificación); sexo; fecha de nacimiento; lugar de nacimiento; nacionalidad; estado civil; alias; apodo; nombres utilizados o nombres falsos; residencia o domicilio actuales y anteriores<sup>93</sup>.

La Decisión EUROPOL a la hora de hablar sobre los datos almacenados relativos a las personas sospechosas de haber cometido o de haber participado en un delito competencia de EUROPOL o que hayan sido condenadas por tal delito, o que sean sospechosas de que cometerán algún delito, teniendo en cuenta los hechos graves que justifiquen tal presunción, prevé que los datos relativos a estas personas sólo podrán incluir los “elementos” como: apellido, apellido de soltera, nombre, alias o nombres

---

información” que sin estar debidamente manejada podría resultar inoportuna, o, podría ocasionar un perjuicio leve o grave a los intereses de EUROPOL o de uno o varios Estados miembros. Al referirse a la acción de difundir la información, se exigía por tanto la actividad de extender, esparcir o divulgar la información de los ficheros clasificados. Ahora bien, el término utilizado que da mayor garantía de protección de los ficheros de datos es el de “revelar”, lo que implica hacer visible o descubrir la información sin que sea necesario que se llegue hasta el punto de su difusión.

<sup>90</sup> Nos referimos al Acto del Consejo de 5 de junio de 2003 que modifica el Acto del Consejo de 3 de noviembre de 1998 por el que se adoptan normas sobre protección del secreto aplicables a la información de EUROPOL, 2003/C 152/01.

<sup>91</sup> Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 999/1999 de 11 de junio y publicado en el BOE de 25 de junio de 1999.

<sup>92</sup> Art. 14.1 Decisión del Consejo de 6 de abril de 2009 por la que se crea la Oficina Europea de Policía, EUROPOL, 2009/371/JAI.

<sup>93</sup> Véase la clasificación que ofrece la Decisión del Consejo 2009/365/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, especialmente el Art.6, “Datos personales contenidos en los ficheros de trabajo de análisis”.

utilizados; fecha y lugar de nacimiento; nacionalidad, sexo; y en la medida en que sea necesario, otras características útiles para su identificación, en particular rasgos específicos, objetivos y permanentes<sup>94</sup>, es decir el aspecto físico y sus características: fisonomía y como rasgos característicos los señales, cicatrices, tatuajes, etc<sup>95</sup>. Es importante subrayar que solamente se hace referencia a las clases de datos que se pueden tratar sin especificar cuál sería el nivel de clasificación y de seguridad que se les aplica, en tanto que son datos personales que identifican con facilidad a una persona.

Con respecto a la segunda categoría de personas que se catalogan como víctimas o posibles víctimas, el conjunto de datos<sup>96</sup> que se pueden almacenar son: las indicaciones personales<sup>97</sup>; los medios de identificación<sup>98</sup>, así como los datos de identificación de la víctima; datos especiales: motivos por los que ha sufrido el delito; los daños sufridos, tanto físicos como financieros, psicológicos u otros; el anonimato que debe garantizarse<sup>99</sup> y la posibilidad de comparecer ante los Tribunales.

En la tercera categoría de personas a las que hace referencia la Decisión EUROPOL apunta hacia los posibles testigos de los delitos en investigaciones sobre los delitos considerados o en una futura causa penal. En este caso se podrán almacenar los datos ya enunciados como: indicaciones personales y medios de identificación, así como la información relacionada con los delitos, proporcionada por tales personas, incluida la información sobre sus relaciones con otras personas incluidas en el fichero de trabajo de análisis; el anonimato que ha de garantizarse; garantías y garantes de protección; nueva identidad, así como la posibilidad de comparecer ante los Tribunales<sup>100</sup>.

---

<sup>94</sup> Art. 12 de la Decisión EUROPOL que se refiere al "Contenido del sistema de información de EUROPOL".

<sup>95</sup> Decisión del Consejo 2009/365/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, art. 6, ap. 2 letra b.

<sup>96</sup> Decisión del Consejo 2009/365/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, Art.6, p.4: "Datos personales contenidos en los ficheros de trabajo de análisis".

<sup>97</sup> Como indicaciones personales están catalogados los siguientes datos personales: apellidos actuales y anteriores; nombres actuales y anteriores; apellido de soltera; sexo; fecha de nacimiento; lugar de nacimiento; nacionalidad; estado civil; residencia o domicilio actuales o anteriores.

<sup>98</sup> En este caso, como medios de identificación serán solo los datos de los documentos de identidad; los números de documento nacional de identidad y del pasaporte y, si procede, los números de identificación nacionales.

<sup>99</sup> El anonimato que se debe garantizar a las víctimas forma parte de un conjunto de técnicas de protección de las víctimas, testigos o peritos en casos criminales. A la hora de facilitar medios de prueba con respecto a un daño sufrido por una acción criminal, la víctima se transforma en "testigo" y es deber del Estado proteger a las víctimas en lo que respecta a su seguridad e intimidad, siempre que existe un riesgo grave de represalias o claros indicios de una intención clara de perturbar la vida privada (Véase <http://www.institutodevictimologia.com/Formacion11f.pdf>). En una investigación criminal, así como en un juicio penal, la víctima tiene derecho a la protección física y todas las personas que tienen contacto con ella tienen la obligación de guardar la confidencialidad con respecto a la vida privada y a la identidad de la víctima. Si en el desarrollo del proceso penal que implica tanto la etapa de investigación penal así como la etapa de comparecencia ante los tribunales, la vida y la salud de la víctima están en peligro, se aplicarán las técnicas de protección de las víctimas, cambiándole el nombre, el apellido, la fecha y el lugar de nacimiento, el puesto de trabajo.

<sup>100</sup> Decisión del Consejo 2009/365/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, art.6, p. 5: "Datos personales contenidos en los ficheros de trabajo de análisis".

Aunque hemos decidido tratar en esta primera parte (o sea en la primera clasificación como nivel básico), sobre los datos personales con respecto a estas últimas cuatro clases de personas, consideramos que éstas deberán gozar desde un principio del más alto nivel de seguridad, y siendo así creemos que deberán ser clasificados como “*EUROPOL Top Secret-Secreto Riguroso*” aunque se prevé explícitamente que toda la información tratada por EUROPOL o a través de EUROPOL gozará del nivel básico de protección y solo en caso estrictamente necesario y durante el plazo necesario la información que exige medidas de seguridad adicionales estará sometida a un nivel de seguridad de EUROPOL y llevará un marcado específico en tal sentido<sup>101</sup>.

Con respecto a la regla más arriba mencionada, y teniendo en cuenta el hecho de que los datos personales, los ficheros o los documentos que EUROPOL recibe de otro Estado miembro en un caso determinado, se devolverán al Estado miembro que los haya suministrado, o se suprimirán o destruirán cuando ya no sean necesarios para los fines para los que hayan sido almacenados; es más, se suprimirán o destruirán en cualquier caso, tras el cierre de un fichero de trabajo de análisis (Carrera Hernández, 2003: 104). Deducimos que la regla mencionada está huérfana de consecuencias jurídicas para estas clases de personas.

Con la intención de motivar nuestra opinión, hacemos un pequeño comentario a estas dos últimas frases, es decir: “la información tratada por EUROPOL solo en caso estrictamente necesario y durante el plazo necesario estará sometida a un nivel de seguridad de EUROPOL” y “los datos personales, los ficheros o los documentos que EUROPOL recibe de otro Estado miembro se suprimirán o destruirán tras el cierre de un fichero de trabajo de análisis”. El cierre de un fichero de trabajo de análisis supone la finalidad de una investigación penal en un caso concreto y lleva consigo la destrucción del fichero, dado que los datos dejan de ser útiles para los fines para los que han sido almacenados y también es una forma de asegurar la seguridad de estos datos. En una investigación en curso, las víctimas, las posibles víctimas, así como los testigos y los que pueden aportar información con respecto a los delitos graves competencia de EUROPOL, deberán gozar de un alto nivel de seguridad, asegurándose en este sentido el anonimato y poniéndose en marcha todas las medidas de seguridad de que se aplican en casos concretos a estas personas.

Es así que, con respecto a esta clase de personas, la información tratada por EUROPOL exige desde un principio un alto nivel de seguridad hasta el final de la investigación y después de comparecer ante los Tribunales. Hay casos en que la seguridad de estas personas exige estas medidas para un largo periodo de tiempo, aún después de la finalidad de un juicio penal, siendo necesario que estas personas cambien totalmente sus vidas, sus nombres, las fechas y los lugares de nacimiento, el puesto de trabajo, etc. Cualquier dato con respecto a estas personas debe gozar desde un principio

---

<sup>101</sup> 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, art. 10, p.1.

del más alto nivel de seguridad dado que “está en juego” la vida de estas personas así como la vida de sus familiares.

Sabemos que EUROPOL almacena datos personales que pueden ser o no introducidos en ficheros de análisis, datos que en un principio entran en los llamados ficheros temporales. Ahora bien, los datos que otros Estados miembros aportan no se guardan en distintos ficheros para que luego sólo sean transferidos a otro Estado, sino que siempre se almacenan y se tratan con fines de análisis lo que supone que los datos personales se almacenan en ficheros de trabajo con fines de análisis y, en este caso, cada fichero deberá tener una nota que indique la categoría de personas dentro de la que se almacenan, el nivel de seguridad que se les aplica, teniendo en cuenta la necesidad de garantizar la confidencialidad de estos datos.

Al decir que se les aplica el nivel básico de seguridad, no significa que los datos son de menor importancia que los demás o que puedan ser accesibles con facilidad. El nivel básico es el nivel que se aplica a todos los datos a la hora de entrar en la base de datos; luego se les asigna otro nivel de seguridad en función del grado de importancia que la información abarca y pasan a la etapa que llamamos “análisis”.

A la hora de fijar el nivel de seguridad de los datos e introducirlos en los ficheros de trabajo de análisis, los datos almacenados se diferenciarán en función del grado de exactitud o fiabilidad de la información, como también los datos basados en hechos serán diferenciados de los datos basados en opiniones o apreciaciones personales<sup>102</sup>.

A cada nivel de clasificación de los datos se le asigna las medidas de seguridad y, en este caso, es el responsable del fichero el que tiene competencia para imponer la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los Sistemas de Información y que deberá contener como mínimo un ámbito de aplicación del documento con especificación detallada de los recursos protegidos; todo el conjunto normativo de medidas, normas, procedimientos, reglas y estandartes encaminados a garantizar el nivel de seguridad; las funciones y las obligaciones del personal; la estructura de los ficheros con datos de carácter personal y la descripción de los Sistemas de Información que tratan, así como el procedimiento de notificación, gestión y respuesta ante las incidencias y, por último, los procedimientos de realización de copias de respaldo y de recuperación de los datos. Obligatoriamente, el documento se mantendrá actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en el mismo fichero de análisis<sup>103</sup>.

El segundo nivel de clasificación de EUROPOL denominado “*EUROPOL Confidential*”, será aplicable “a la información y al material cuya revelación no autorizada

<sup>102</sup> Decisión del Consejo 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, art. 9.

<sup>103</sup> Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por el Real Decreto 994/1999, de 11 de junio, y publicado en el BOE de 25 de junio de 1999.

pueda causar un perjuicio a los intereses esenciales de EUROPOL, de la UE, o de uno o varios Estados miembros”<sup>104</sup>. En la escalera jerárquica, los datos personales almacenados reciben un mayor grado de seguridad y de confidencialidad, lo que supone que a la hora de motivar la petición de acceso a esta clase de datos, las condiciones que se deben cumplir serán más exigentes.

A este tipo de datos podríamos incorporar los datos personales que se dividen a su vez en las siguientes clases: medios de identificación-documentos de identidad; números de documento nacional de identidad y pasaportes; número de identificación nacional; profesión y captaciones-actividad laboral y profesional actual; actividad laboral y profesional anterior; títulos académicos; aptitudes; captaciones y otros conocimientos; medios de comunicación y medios de transporte que usa<sup>105</sup>.

La segunda clase de datos clasificados como de nivel medio abarca, además de los datos del nivel básico, otras clases de datos que requieren mayor seguridad. Esto es lo que pasa con cada uno de los niveles de seguridad, es decir, los datos que “entran” se clasifican como de nivel básico; después, si se almacenan otros datos que requieren un nivel más alto, es decir, cuando se reúna información con marca de protección de distintos niveles, el nivel de clasificación que se aplique será, como mínimo, tan alto como el de la información protegida en el nivel más alto<sup>106</sup>.

El tercer nivel de clasificación de EUROPOL se denomina “*EUROPOL Secret*” y será aplicable a la “información y al material cuya revelación no autorizada pueda causar un perjuicio grave para los intereses esenciales de EUROPOL, de la UE, o de uno o varios Estados miembros”. Si en el nivel básico y en el nivel medio una acción de revelación no autorizada podría resultar desfavorable o podría ocasionar un perjuicio para los intereses de EUROPOL, de la UE, o de un Estado miembro, en este alto nivel de seguridad el perjuicio se cataloga como “grave”.

Por lo que asumimos que este nivel de seguridad se aplica a las siguientes dos clases de información:

- 1) información económica y financiera: datos financieros (cuentas y códigos bancarios, tarjetas de crédito, etc.); activos líquidos disponibles; acciones y otros activos; datos sobre propiedades; vínculos con sociedades y empresas; contactos bancarios y crediticios; situación fiscal; otra información que indique la forma de gestionar los asuntos financieros de una persona;
- 2) datos sobre el comportamiento: estilo de vida (vida por encima de las posibilidades, por ejemplo) y costumbres; movimientos; lugares de frecuentación;

<sup>104</sup> Acto del Consejo de 5 de junio de 2003 que modifica el Acto del Consejo de 3 de noviembre de 1998 por el que se adoptan normas sobre protección del secreto aplicables a la información de EUROPOL, 2003/C152/01.

<sup>105</sup> Decisión del Consejo 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, art. 6, letra c, d, h.

<sup>106</sup> Decisión 2009/968/JAI, del Consejo de 30 de noviembre de 2009, por la que se adoptan las normas sobre la confidencialidad de la información de EUROPOL, art. 10, p. 4, ap. 4.



armas y otros instrumentos peligrosos; peligrosidad; riesgos específicos como probabilidad de fuga, utilización de agentes dobles; conexiones con personal policial o de aduanas; aspectos y perfiles relacionados con la delincuencia; toxicomanías<sup>107</sup>.

El último nivel de clasificación de EUROPOL se denomina “EUROPOL Top Secret-EUROPOL Secreto Riguroso”, y es el más alto nivel de seguridad que se puede aplicar a los datos de EUROPOL. Este nivel será aplicable a la “información y material cuya revelación no autorizada pueda causar un perjuicio excepcionalmente grave a los intereses esenciales de EUROPOL, de la UE, o de uno o varios Estados miembros<sup>108</sup>”.

Consideramos que los datos almacenados en los ficheros de análisis que gozarán del más alto nivel de seguridad de EUROPOL serán:

- 1) relativos a las actividades delictivas en las que es competente EUROPOL: condenas anteriores; presunta implicación en actividades delictivas; *modus operandi*; instrumentos efectivos o posibles para preparar o cometer delitos; grupo u organización delictiva a la que pertenece y posición en el grupo u organización; situación y función en la organización delictiva; ámbito geográfico de las actividades delictivas, material recogido durante una investigación, como imágenes fotográficas y en video<sup>109</sup>;
- 2) datos que releven el origen racial; las opiniones políticas; las convicciones religiosas u otras convicciones; datos relativos a salud o a la vida sexual<sup>110</sup>;
- 3) información sobre identificación forense como impresiones dactilares; resultados de la evaluación del ADN<sup>111</sup>, características de la voz; grupo sanguíneo, información dental;
- 4) referencias a otras bases de datos en que haya almacenados datos sobre la persona: EUROPOL; Cuerpos de policía y aduanas; otros cuerpos de seguridad; organizaciones internacionales; entidades públicas; entidades privadas;
- 5) cualquier dato con respecto a las víctimas o, posibles víctimas, testigos o posibles testigos.

En cada Estado miembro, cada nivel de seguridad que se aplica a los datos gozará de sus propias medidas de seguridad que deberá contener el “documento de

<sup>107</sup> Decisión del Consejo 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, art. 6, letras e, f.

<sup>108</sup> Decisión 2009/968/JAI del Consejo, de 30 de noviembre de 2009, por la que se adoptan las normas de confidencialidad de la información de EUROPOL, art. 10, p. 4.

<sup>109</sup> Decisión del Consejo 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, art. 6, letra j.

<sup>110</sup> Estos datos de carácter personal están calificados por el C108 como categorías particulares de datos que no podrían tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas.

<sup>111</sup> Todas estas únicamente con fines de identificación y sin información que caracterice la personalidad.

seguridad". Se establecerá una Auditoría interna o externa que deberá verificar el cumplimiento de las normas de los procedimientos e instrucciones vigentes en materia de seguridad de los datos. Los Informes de auditoría serán analizados por el responsable de seguridad competente que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos<sup>112</sup>.

La eficacia de la acción policial depende en gran medida de la información policial en tanto que herramienta principal en la elaboración de actividades de prevención y represión de acciones criminales cada vez más globalizadas y que solo pueden combatirse debidamente mediante el desarrollo de los mecanismos de colaboración internacional entre los cuerpos policiales.

## **Bibliografía**

- ARENAS RAMIRO, M.: 2006, *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch.
- BONN M.: 2007, "El Programa de la Haya. El Espacio de Libertad, Seguridad y Justicia en la Unión Europea", en *El Derecho penal de la Unión Europea. Situación actual y perspectivas de futuro*, Universidad de Castilla-La Mancha.
- CARRERA HERNÁNDEZ, F.J.: 2003, *La cooperación policial en la Unión Europea: Acervo Schengen y Europol*, Madrid, Colex.
- GARCÍA BEATO, M. J.: 1997. "El flujo internacional de datos personales", en *La Protección del Derecho a la Intimidad de las personas*, Madrid, Cuadernos de Derecho Judicial.
- LASAGABASTER HERRARTE I.: 2004, *Convenio Europeo de Derechos Humanos, Comentario Sistemático*, Madrid, Civitas.
- MARTÍNEZ MARTÍNEZ, R.: 2001, *Tecnologías de la información, la policía y la Constitución*, Valencia, Tirant lo Blanch.
- PAVÓN PÉREZ, A: 2001-2002, "La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales", *Anuario de la Facultad*.

---

<sup>112</sup> Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999 de 11 de junio y publicado en el BOE de 25 de junio de 1999.





[www.icps.cat](http://www.icps.cat)