



CONSEJO GENERAL DEL PODER JUDICIAL
ESCUELA JUDICIAL



Red Europea de Formación Judicial (REFJ)
European Judicial Training Network (EJTJN)
Réseau Européen de Formation d'ici (REFJ)

MÓDULO III

TEMA 9

El Principio de Disponibilidad: Antecedentes Penales y Convenio de Prüm

5ª Edición
2013



AUTORES

Fernando Martínez Pérez

Magistrado. Juzgado de Instrucción nº 7 de Sevilla

María Poza Cisneros

Magistrada de la Audiencia Provincial de Murcia



Con el apoyo financiero del Programa de Justicia Penal de la Unión Europea
With the financial support from the Criminal Justice Programme of The European Union
Avec le soutien financier du Programme de Justice Pénale de l'Union Européenne

NIVELES

NIVEL I: TEMA

NIVEL II: PARA SABER MAS

NIVEL III: DOCUMENTACIÓN DE REFERENCIA

NIVEL IV: ESPECIFICACIONES PARA ESPAÑA

NIVEL I: TEMA

SUMARIO

1. El principio de disponibilidad

- 1.1. Definición
- 1.2. Transposición del principio

2. El Tratado de Prüm

- 2.1. Origen, naturaleza y ámbito de aplicación
- 2.2. Contenido
 - 2.2.1. Acceso automatizado a ficheros nacionales
 - 2.2.1.1. Perfiles de ADN
 - 2.2.1.2. Datos dactiloscópicos
 - 2.2.1.3. Datos de vehículos
 - 2.2.1.4. Otros datos
 - 2.2.2. Medidas de prevención de atentados terroristas
 - 2.2.2.1. Transmisión de información
 - 2.2.2.2. Escolta de seguridad en los vuelos
 - 2.2.3. Medidas para la lucha contra la migración ilegal
 - 2.2.3.1. Envío de asesores en materia de documentación
 - 2.2.3.2. Apoyo en casos de repatriación
 - 2.2.4. Otras formas de cooperación
 - 2.2.4.1. Patrullas comunes y otras formas de intervención conjunta
 - 2.2.4.2. Cruce de frontera
 - 2.2.4.3. Asistencia en caso de grandes eventos, catástrofes y accidentes graves
 - 2.2.4.4. Cooperación previa petición
 - 2.2.5. Disposiciones sobre protección de datos de carácter personal
 - 2.2.5.1. Definiciones
 - 2.2.5.2. Nivel de protección de datos
 - 2.2.5.3. Principio de vinculación a fines y otros límites de utilización y tratamiento de datos
 - 2.2.5.4. Garantías de exactitud, actualidad y duración del almacenamiento de los datos
 - 2.2.5.5. Medidas técnicas y organizativas para garantizar la protección de los datos y su seguridad
 - 2.2.5.6. Documentación y registro

3. La parcial incorporación del Tratado de Prüm al marco jurídico de la Unión Europea

- 3.1. La Decisión JAI/615/2008
- 3.2. La Decisión JAI/616/2008

4. El principio de disponibilidad en el Programa de Estocolmo

5. Antecedentes penales

- 5.1. Introducción**
- 5.2. Decisión Marco 2008/675/JAI**
- 5.3. Decisión Marco 2009/315/JAI**
- 5.4. Decisión 2009/316/JAI**

1. El principio de disponibilidad

1.1. Definición

En el **Programa de La Haya**¹, de 10 de mayo de 2005, el Consejo Europeo “reafirma el carácter prioritario que atribuye a la creación de un espacio de libertad, seguridad y justicia, en respuesta a una inquietud fundamental de los pueblos de los Estados que constituyen la Unión”. Sus orientaciones específicas se desarrollan en cuatro capítulos, relativos a la consolidación de la libertad, de la seguridad, al reforzamiento de la justicia y al desarrollo de las relaciones exteriores. El segundo de dichos capítulos (“Consolidación de la seguridad”) se refiere a la mejora del intercambio de información, a la prevención y lucha contra el terrorismo, a la cooperación policial, a la gestión de crisis internas de la Unión Europea con repercusiones transfronterizas, a la cooperación operativa, a la prevención de la delincuencia y, brevemente, a la delincuencia organizada, la corrupción y la estrategia en la lucha contra la droga. En relación con la mejora del intercambio de la información, se introduce, por vez primera, una definición del principio de disponibilidad, como instrumento innovador del intercambio transfronterizo de información policial, cuya implantación se impone a fecha fija, 1 de enero de 2008, y en términos categóricos.

El **principio de disponibilidad** se define en el Programa de La Haya como aquél que permite que, en todo el territorio de la Unión, un funcionario de policía de un Estado miembro que necesite información para llevar a cabo sus obligaciones pueda obtenerla de otro Estado miembro y que el organismo policial del otro Estado miembro que posea dicha información la facilitará para el propósito indicado, teniendo en cuenta el requisito de las investigaciones en curso en dicho Estado.

El principio de disponibilidad garantiza que la Policía de un EM, en el cumplimiento de sus funciones de investigación, puede obtener información de la Policía de otro EM.

¹ Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 10 de mayo de 2005, «Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia» (COM (2005)184 final – Diario Oficial C 236 de 24.9.2005).

El propio Programa de La Haya anticipa determinadas **condiciones mínimas** a las que habrían de ajustarse las propuestas que invitaba a la Comisión a presentar, para la aplicación del principio:

- El intercambio solamente puede tener lugar para el cumplimiento de tareas legales.
- Debe garantizarse la integridad de los datos que deban intercambiarse.
- Las fuentes de información han de ser protegidas y la confidencialidad de los datos, en todas las etapas del intercambio, garantizada.
- Ulteriormente, deben aplicarse normas comunes para el acceso a los datos y normas técnicas comunes.
- Debe supervisarse el respeto de la protección de los datos y garantizarse un adecuado control previo y posterior al intercambio de información.
- Debe garantizarse la protección contra el uso indebido de los datos personales y el derecho a la corrección de los datos personales incorrectos.

Se precisaba, igualmente, que los métodos de intercambio de información deberían hacer pleno uso de las **nuevas tecnologías** y adaptarse a cada tipo de información, si procediere, a través del acceso recíproco a las bases de datos nacionales o la interoperabilidad de las mismas, o del acceso directo (en línea), incluso para Europol, a las bases de datos centrales existentes de la UE, tales como el SIS. Sólo deberían crearse nuevas bases de datos europeas centralizadas sobre la base de estudios que hubieran demostrado su valor añadido.

La nominación y reafirmación del principio de disponibilidad, en el Programa de La Haya, estuvo precedida de una **creciente preocupación** por mejorar los intercambios de información entre las autoridades encargadas de garantizar el cumplimiento de la ley, de la que son expresión diversas Comunicaciones de la Comisión², avivada, como ya sucediera con el principio de reconocimiento mutuo con ocasión del 11-S, por los atentados terroristas de Madrid, en marzo de 2004. De hecho, ya desde el Consejo Europeo de Tampere, de 1999, se perseguía intensificar la cooperación policial, aduanera y judicial, y desarrollar una política coordinada en materia de asilo, inmigración y controles en las fronteras exteriores.

² Comunicación de la Comisión al Parlamento Europeo y al Consejo para “Reforzar la cooperación policial y aduanera en la Unión Europea”, de 18 de mayo de 2004 (COM 2004/376 final, no publicada en el D.O.) y Comunicación de la Comisión al Consejo y al Parlamento Europeo “sobre mejora del acceso a la información por parte de las autoridades encargadas de garantizar el cumplimiento de la Ley”, de 16 de junio de 2004 (COM 2004/429 final, no publicada en el D.O.).

Con anterioridad, los principales instrumentos que habían intentado dar respuesta a esta ahora recobrada inquietud acerca de las debilidades del intercambio de información policial eran³:

- El Convenio de aplicación del Acuerdo de Schengen de 1990. Su artículo 39 prevé el intercambio de información entre los servicios de policía que lo soliciten, pero no obliga a los Estados miembros a contestar.
- El Convenio Europol de 1995 y sus protocolos. De conformidad con el artículo 2, el objetivo de Europol es mejorar la eficacia de los servicios competentes de los Estados miembros y la cooperación entre los mismos, con vistas a la prevención y lucha contra el terrorismo y otras formas graves de delincuencia internacional y organizada.
- La iniciativa del Reino de Suecia relativa a un proyecto de Decisión Marco sobre simplificación del intercambio de información e inteligencia, que intentaba mejorar el mecanismo creado por el Convenio de Schengen, conseguir una mayor armonización del marco jurídico en el que se produce el intercambio de datos y reducir los tiempos de respuesta y que cristalizaría en la DM 2006/960/JAI.

Paralelamente, además, se estaba gestando el Tratado que sería firmado en Prüm, el 27 de mayo de 2005, por siete Estados miembros, con pretensión de incorporar sus disposiciones al marco jurídico de la Unión Europea en el plazo máximo de tres años. Este Tratado, al que nos referiremos por extenso más adelante, pretendía una cooperación reforzada que ofreciera mejor respuesta, entre otras, a las necesidades de intercambio de información policial, orientada, particularmente, a la lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal.

1.2. Transposición del principio

El Plan de Acción del Consejo y la Comisión por el que se aplica el Programa de La Haya⁴ confirmaba la presentación de la propuesta que permitiría la traducción normativa del principio de disponibilidad, acompañada de otra propuesta, sobre protección de datos personales. La primera iniciativa, representada por la **Propuesta de DM del Consejo, de 12 de octubre de 2005**⁵, sobre el intercambio de información en virtud del principio de disponibilidad, sin embargo, no prosperó.

³ Según la EM de la fallida Propuesta de DM del Consejo de 12 de octubre de 2005 a que nos referimos en el siguiente apartado.

⁴ Adoptado por el Consejo de Justicia e Interior de 2 y 3 de junio de 2005.

⁵ COM/2005/0490 final.

Mejor fortuna tuvo, a iniciativa sueca, origen del que toma el nombre por el que es conocida, la que sería **DM 2006/960/JAI de 18 de diciembre de 2.006**⁶, considerada, por algunos autores, como una primera aproximación a la puesta en marcha del principio de disponibilidad, superando la primitiva etapa bilateral, e, incluso, la que podríamos denominar “etapa institucional”, en la que la mejora de la información se confiaba a agencias o estructuras europeas como Europol. La Decisión Marco se refiere a la “simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea”. En su Exposición de Motivos, se introduce expresamente, entre otras cuestiones, el que será recurrente objetivo en la materia: alcanzar el correcto equilibrio entre dos imperiosas necesidades:

- El intercambio rápido y eficaz de información e inteligencia entre los servicios de seguridad de los Estados miembros, imprescindible para la lucha contra la delincuencia transfronteriza.
- La protección de datos personales, libertades fundamentales, derechos humanos y libertades individuales.

La idea básica que inspira la DM es la libre circulación de información e inteligencia entre las autoridades encargadas de garantizar el cumplimiento de la ley. En las definiciones auténticas que incorpora, amplias, con el objetivo de garantizar que la libre circulación no se vea obstaculizada por diferencias en la organización nacional:

- “Servicio de seguridad competente” es la autoridad nacional policial, aduanera u otra, autorizada según el Derecho interno a descubrir, prevenir e investigar delitos y actividades delictivas y a ejercer la autoridad y adoptar medidas coercitivas en el contexto de esas actividades. Las agencias o unidades que traten especialmente cuestiones de seguridad nacional no quedan cubiertas por el concepto, que será aclarado, mediante declaración siempre modificable, por cada Estado miembro.
- “Investigación criminal” es la fase del procedimiento dentro de la cual los servicios de seguridad o las autoridades judiciales competentes, incluido el Ministerio Fiscal, adoptan medidas para el establecimiento y averiguación de los hechos, los sospechosos y las circunstancias en relación con uno o varios actos delictivos concretos comprobados. La Decisión no se limita, por tanto, a las fases preprocesales y su interés supera, en consecuencia, el ámbito de la cooperación policial.

⁶ Publicada en el D.O.L 386, de 29 de diciembre de 2.006, con una rectificación en el D.O. L 75 de 15 de marzo de 2007.

- “Operación de inteligencia criminal” es la fase del procedimiento que no ha alcanzado aún la fase de investigación criminal, dentro de la cual el Derecho interno autoriza a un servicio de seguridad competente a recoger, tratar y analizar información sobre delitos o actividades delictivas para establecer si se han cometido actos delictivos concretos o se pueden cometer en el futuro.
- “Información y/o inteligencia” es todo tipo de información o datos en poder de:
 - Los servicios de seguridad, ya definidos.
 - Autoridades públicas o entes privados, de la que puedan disponer los servicios de seguridad sin tener que utilizar medidas coercitivas.

En cuanto a la distinción entre “información” e “inteligencia”, los tratadistas vienen entendiendo que la inteligencia criminal es el producto resultante de la recolección, procesamiento, integración, análisis, evaluación e integración de la información disponible y su misión establecer los patrones criminales propios de organizaciones o empresas dedicadas a la comisión de delitos: formas de operar, estructuras, miembros, recursos y causas, entre otros aspectos relevantes.

Respecto de su ámbito de aplicación, la DM impone a los Estados miembros la obligación de:

- Garantizar que la información y/o inteligencia puedan suministrarse a petición del servicio de seguridad competente que lleve a cabo una investigación criminal o una operación de inteligencia criminal, sin supeditarla a condiciones más estrictas que las aplicables a escala nacional.
- Solicitar, cuando conforme al derecho interno, sea exigible recabar autorización judicial para acceder a la información de que se trate o para intercambiarla, a través de los servicios de seguridad del Estado requerido, dicha autorización, que habrá de otorgarse o denegarse con aplicación de los mismos criterios que se aplicarían a un asunto exclusivamente interno.

En la solicitud, debe exponerse el fin para el que se solicita la información o inteligencia y la vinculación entre éste y la persona objeto de aquéllas y se establecen breves plazos, en función de la urgencia, de 8 horas a 14 días, con obligación de comunicar los motivos del retraso.

Se introducen, no obstante, determinadas matizaciones, límites y prohibiciones:

- No se impone, a los Estados miembros, obligación de recoger y almacenar información, con el fin de facilitarla a los servicios de seguridad de otro Estado miembro. Se trata, pues, de facilitar el acceso a la información “existente”, ya disponible para el Estado requerido.

- No se impone, a los Estados miembros, obligación de facilitar información e inteligencia, para su utilización como prueba ante la autoridad judicial, ni confiere derecho alguno a utilizarlas con ese fin, si bien puede destinarse a ello, con consentimiento del Estado miembro que haya facilitado la información y/o la inteligencia, empleando, si fuere necesario, los instrumentos de cooperación judicial, salvo que, desde el primer momento, el Estado requerido ya hubiese anticipado que accedía al uso de la información transmitida con fines de prueba.
- No se impone al Estado miembro requerido de información o inteligencia su obtención mediante medidas coercitivas, definidas según su legislación interna.
- No es posible transmitir información y/o inteligencia a un Estado miembro cuando se ha obtenido de otro Estado miembro o de un tercero, sujeta a la regla de especialidad, salvo autorización del Estado que la proporcionó.
- Se prohíbe solicitar más información que la necesaria para descubrir, prevenir o investigar un delito.
- Se imponen estrictas normas sobre protección de datos y confidencialidad de la información y/o inteligencia confidencial suministrada.
- Se establecen motivos para no comunicar información o inteligencia.
 - Razones potestativas
 - Cuando por razones de hecho se suponga que el suministro:
 - Perjudicaría intereses esenciales en materia de seguridad nacional del Estado miembro requerido, o
 - comprometería el éxito de una investigación en curso o de una operación de inteligencia criminal o la seguridad de las personas, o
 - sería claramente desproporcionado o irrelevante para el fin que persigue.
 - Cuando la solicitud se refiera a un delito castigado con pena de prisión igual o inferior a un año con arreglo a la legislación del Estado miembro requerido.
 - Razones imperativas: Cuando la autoridad judicial competente no ha autorizado el acceso o el intercambio de la información solicitada.

La traducción normativa del principio de disponibilidad se encuentra en:

- La DM 2006/960/JAI (“Iniciativa sueca”).
- El Tratado de Prüm.
- La Decisión JAI/615/2008.

de ADN, impresiones dactilares, balística, registros de vehículos y números de teléfono, datos mínimos de personas contenidos en registros civiles, materias muchas de ellas ya abordadas por el Tratado de Prüm. El Comité del Artículo 36 de TUE (también denominado CATS), como grupo de trabajo del Consejo, que tenía como misión coordinar a los grupos de trabajo competentes en el ámbito del tercer pilar, encomendó la ejecución de este objetivo de estudio al Grupo Multidisciplinario de Delincuencia Organizada (GMD).

En paralelo, como hemos anticipado, se gestaba la incorporación del **Tratado de Prüm** al marco jurídico comunitario, datando la iniciativa, a tal fin, de 15 de enero de 2007⁷ y cristalizando, finalmente, en las **Decisiones JAI/615/2008 y JAI/616/2008**, de 23 de junio, en las que convergen la voluntad de “comunitarizar” el Tratado de Prüm que anunciaron sus signatarios y la exigencia de articular jurídicamente el principio de disponibilidad incorporado al Programa de La Haya, como viene a reconocer la Exposición de Motivos de la primera de las citadas Decisiones, al “descubrir”, en el Tratado, los contenidos que permitirían cumplir los requisitos sustantivos del Programa dentro de los plazos fijados en él. De estos instrumentos normativos nos ocuparemos en sucesivos apartados independientes.

Por otro lado, agotado, en 2009, el Programa quinquenal de La Haya, el Programa de Estocolmo (2009_2014), en un nuevo escenario político y jurídico, coincidente con la entrada en vigor del Tratado de Lisboa, anuncia nuevos desarrollos del principio de disponibilidad que, en parte, inspira la estrategia comunitaria en relación con la información sobre antecedentes penales, regida ya, sin embargo, por el principio de reconocimiento mutuo, avanzando, conceptualmente, ya, en el último apartado, en el objeto del Módulo siguiente.

2. El Tratado de Prüm

2.1. Origen, naturaleza y ámbito de aplicación.

El 27 de mayo de 2005 siete Estados Miembros de la UE (Bélgica, Alemania, España, Francia, Luxemburgo, Holanda y Austria) firmaron, en la ciudad alemana de Prüm, el tratado del mismo nombre “relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal”, que establece diversas medidas para mejorar la cooperación policial y, por extensión, también la cooperación judicial.

⁷ Publicada en el D.O. de 28 de marzo de 2007.

Los **precedentes** de esta iniciativa hay que buscarlos en el Acuerdo de Schengen de 1.985 y el Convenio de aplicación de 1.990, conocidos como “Schengen I” y Schengen II”, hasta el punto de que el Tratado que comentamos es también conocido, con manifiesta impropiedad, como Schengen III o Schengen Plus. Inicialmente, fue promovido sólo por Alemania, Bélgica y Luxemburgo, como una vía de cooperación reforzada a la que se sumaron otros cuatro Estados. Se encuentra abierto a la **adhesión** de cualquier Estado miembro y, posteriormente, se sumaron Bulgaria, Estonia, Finlandia, Hungría, Rumania, Eslovaquia y Eslovenia. Grecia, Italia, Portugal y Suecia comunicaron al Consejo Europeo su voluntad de adherirse al Convenio. A través de acuerdos específicos y ya en relación con las Decisiones que incorporan al marco jurídico de la Unión Europea parte de sus previsiones, participan de algunas de ellas Noruega e Islandia. El 5 de diciembre de 2006 fue firmado el Acuerdo Técnico de Ejecución del Tratado de Prüm, previsto en el artículo 44 del mismo.

En su propia génesis, es manifiesta la vocación del tratado de transposición al marco jurídico de la UE. Su naturaleza jurídica, no obstante, es la de un **tratado tradicional** que establece bases para una cooperación gubernamental al margen del marco comunitario establecido para la cooperación policial y judicial, en el contexto del espacio de libertad, seguridad y justicia. Se ha calificado de instrumento de **“falsa/verdadera cooperación reforzada”** (ZILLER):

- “Falsa” cooperación reforzada, desde el punto de vista formal, porque el número de Estados inicialmente firmantes es inferior al de ocho exigido, en aquella fecha, en el Tratado de la UE.
- “Verdadera” cooperación reforzada, desde el punto de vista material, porque su contenido se corresponde con uno de los objetivos del artículo 29 del Tratado de la UE, “la prevención de la delincuencia, organizada o no, la lucha contra este fenómeno (en particular el terrorismo)”.

En efecto, el **objetivo** del Tratado de Prüm, que se asume con vocación pionera, es el de intensificar, en un espacio de libre circulación de personas, la cooperación de los Estados miembros, en la lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, tres objetivos que se encuentran también en el Programa de La Haya. En materia de terrorismo, por ejemplo, destaca la coincidencia en avanzar posibilidades de ofrecer información no solicitada, confirmándose, en general, un desarrollo paralelo, a nivel comunitario y en el Tratado, de diversas materias, que generó notable controversia.

Si bien la referencia al principio de disponibilidad no se recoge de forma explícita, la consecución de este objetivo de máxima cooperación, en especial en estas tres áreas, se vincula, desde los primeros párrafos introductorios, al instrumento de un “mejor intercambio de información”. Este objetivo se vincula al propósito de incorporar el régimen del Tratado al marco jurídico de la Unión Europea, para conseguir una mejora global a ese nivel y creando a tal fin las bases jurídicas y técnicas necesarias. Todo ello, “dentro del respeto de los derechos fundamentales, tal y como se recogen en la Carta de Derechos Fundamentales de la Unión Europea, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y las tradiciones constitucionales comunes de los Estados participantes”, y anticipando la preocupación por la garantía de un nivel adecuado de protección de datos de carácter personal en la Parte receptora, paralela al anuncio de otros acuerdos que posibiliten la consulta automatizada de datos de otras bases.

Objetivo del Tratado de Prüm: cooperación más intensa en la lucha contra:

- El terrorismo.
- La delincuencia transfronteriza.
- La migración ilegal

Respecto de su **relación con el Derecho comunitario y con otros instrumentos normativos**, el Tratado prevé:

- La puesta en marcha de una iniciativa para trasladar sus disposiciones al marco jurídico de la Unión Europea en el plazo máximo de tres años desde su entrada en vigor.
- La información periódica por las Partes Contratantes, conjuntamente, al Consejo de la Unión Europea y a la Comisión, acerca de los avances en la cooperación.
- La aplicación de sus disposiciones supeditada a su compatibilidad con el derecho de la Unión Europea.
- La no afectación de los derechos y obligaciones contenidos en otros convenios bilaterales o multilaterales ya existentes, conservando las Partes Contratantes la facultad de aplicarlos en sus relaciones mutuas, si bien con prevalencia, en caso de conflicto, de lo dispuesto en el Tratado.

El Tratado se **estructura** en ocho capítulos:

- I. Parte General.
- II. Perfiles de ADN, datos dactiloscópicos y otros datos.

- III. Medidas para la prevención de atentados terroristas.
- IV. Medidas para la lucha contra la migración ilegal.
- V. Otras formas de cooperación.
- VI. Disposiciones generales.
- VII. Disposiciones generales sobre protección de datos.
- VIII. Disposiciones de aplicación y disposiciones finales.

2.2. Contenido

2.2.1. Acceso automatizado a ficheros nacionales.

El Tratado, en su Capítulo II, artículos 2 a 15, se refiere a tres tipos de ficheros nacionales, permitiendo, a las autoridades de los demás Estados Parte, un acceso inmediato a la información que conste en los mismos, mediante índices de referencia, a través de puntos de contacto. Los tres ficheros contemplados se refieren a los siguientes datos:

2.2.1.1. Perfiles de ADN.

- Creación de ficheros nacionales de análisis de ADN
 - Las Partes se comprometen a la creación y mantenimiento de ficheros nacionales de ADN para los fines de la persecución de los delitos (no de prevención, como se contempla respecto de otros datos menos sensibles).
 - El tratamiento de los datos almacenados en los ficheros en virtud del Tratado se llevará a cabo con arreglo al derecho interno vigente para cada tipo de tratamiento, sin perjuicio de las demás disposiciones del propio Tratado.
 - Las Partes garantizan la disposición de índices de referencia relativos a los datos contenidos en tales ficheros. Estos índices, no obstante, contendrán, exclusivamente, perfiles de ADN, obtenidos a través de su parte no codificante y una referencia, sin que incorporen datos que permitan identificar directamente a la persona concernida. Sin embargo, las denominadas "huellas abiertas" o índices de referencia que no pueden atribuirse a persona determinada, deben poder ser reconocidos como tales.
 - Cada Parte designará los ficheros nacionales de análisis de ADN a los que le son de aplicación los artículos 2 a 6 y las condiciones para su consulta automatizada.

- Consulta automatizada de perfiles de ADN
 - A través de los puntos de contacto nacionales, las Partes permitirán el acceso a los índices de referencia de sus ficheros de análisis de ADN. El acceso autorizado permite la consulta automatizada mediante comparación de perfiles, para casos concretos y con arreglo al Derecho de la Parte contratante que realice la consulta.
 - Si, como resultado de ésta, se comprobase una coincidencia entre perfil transmitido y almacenado en el fichero de la Parte receptora, el punto nacional requirente recibirá de forma automatizada información sobre la existencia de tal concordancia y su referencia. También se comunicará de manera automatizada la ausencia de coincidencia. El sistema responde, pues, al modelo “hit/ no hit”.
- Comparación automatizada de perfiles de ADN, a efectos de contrastar los perfiles de ADN de sus huellas abiertas con todos los perfiles contenidos en los índices de referencia de los demás ficheros nacionales. Se trata, obviamente, de procurar, de este modo, reducir el número de huellas abiertas, por lo que, de comprobarse alguna coincidencia, se comunicará sin demora al punto de contacto nacional de la otra Parte. La transmisión para estos fines sólo tendrá lugar en los casos previstos en el derecho interno de la Parte requirente.
- Obtención de material genético molecular y transmisión de perfiles de ADN. En los casos en que no se disponga de perfil de ADN de una persona determinada que se encuentre en el territorio de la Parte requerida, ésta deberá prestar asistencia judicial mediante la obtención y el análisis de material genético molecular de dicha persona y la transmisión del perfil resultante, siempre que concurren los tres requisitos siguientes:
 - Respecto de la Parte requirente:
 - Comunicación del fin del requerimiento.
 - Presentación de orden o declaración de investigación de la autoridad competente exigible con arreglo a su derecho interno, de la que se desprenda que se cumplirían los requisitos para la obtención y análisis de material genético molecular si esa persona concreta se encontrara en el territorio de la Parte Contratante requirente.
 - Respecto de la Parte requerida, cumplimiento de los requisitos para este objeto con arreglo a su derecho interno.

2.2.1.2. Datos dactiloscópicos.

- Las Partes garantizan la disposición de índices de referencia relativos a los datos contenidos en los sistemas automatizados nacionales de identificación dactiloscópica creados para los fines de la prevención y persecución de los delitos. A diferencia del caso anterior, se presupone que todos los Estados disponen ya de estos ficheros.
- Estos índices, no obstante, contendrán, exclusivamente, datos dactiloscópicos y una referencia, sin que incorporen datos que permitan identificar directamente a la persona concernida. Sin embargo, las denominadas "huellas abiertas" o índices de referencia que no pueden atribuirse a persona determinada, deben poder ser reconocidos como tales.
- Consulta automatizada de datos dactiloscópicos, con un sistema similar al previsto para los perfiles de ADN, también a través de puntos de contacto nacionales. La conexión definitiva de un dato dactiloscópico con un índice de referencia de la Parte Contratante que mantenga el fichero se efectuará por el punto de contacto nacional que realice la consulta sobre la base de los índices de referencia comunicados de forma automatizada que sean necesarios para la atribución definitiva.
- Si en el curso de la consulta automatizada, se comprueba la concordancia de datos dactiloscópicos, la transmisión de otros datos de carácter personal disponibles relativos a los índices de referencia y demás informaciones se efectuará con arreglo al derecho interno de la Parte Contratante requerida, incluidas sus disposiciones relativas a la asistencia judicial.

2.2.1.3. Datos de vehículos.

Con arreglo al derecho interno de la Parte Contratante que realice la consulta, con fines, más amplios, de prevención y persecución de delitos y de lo que denomina, parece que en términos alternativos, " persecución de infracciones que sean competencia de los tribunales o de las fiscalías en el territorio de la Parte Contratante que realice la consulta", y prevención de amenazas para la seguridad y el orden público, a través de puntos de contacto nacionales, se podrá consultar, de manera automatizada, los datos existentes en los registros nacionales de matriculación de vehículos, en muchos Estados a cargo de autoridades no policiales, en casos concretos y siempre en relación con un número completo de identificación de un vehículo o matrícula completa:

- Datos de los propietarios y usuarios.
- Datos de los vehículos.
- y respecto de un número completo de identificación o matrícula completa de un vehículo, pudiendo referirse la consulta a los datos de los propietarios o usuarios y a los datos del vehículo.

2.2.1.4. Otros datos

Además de las tres categorías específicas anteriores, se prevén, también a través de puntos de contacto nacionales, con fines de **prevención** de delitos y amenazas para la seguridad y el orden público, en relación con **grandes eventos transfronterizos, en particular en el ámbito del deporte⁸ o de las reuniones del Consejo Europeo**:

- Transmisión de informaciones de carácter no personal, previa petición o a iniciativa propia de la parte transmitente.
- Transmisión de datos de carácter personal, con los mismos fines, cuando la existencia de condenas firmes o de otras circunstancias justifiquen la presunción de que estas personas van a cometer un delito con motivo del evento o suponen una amenaza para la seguridad y el orden públicos, en la medida en que la transmisión de tales datos sea admisible con arreglo al derecho interno de la Parte Contratante transmitente, también tanto previa petición como a iniciativa propia. Estos datos solo podrán ser tratados para los fines establecidos y para el evento concreto para el que se comunicaron, suprimiéndose inmediatamente una vez cumplidos los fines que justificaron la transmisión, cuando no puedan ya cumplirse o, en todo caso, en el plazo máximo de un año.

2.2.2. Medidas de prevención de atentados terroristas.

2.2.2.1. Transmisión de información:

A través de puntos de contacto nacionales, con fines de prevención de atentados terroristas, en casos concretos, con arreglo a derecho interno y posibilidad de imponer condiciones acerca del empleo de los datos a la autoridad receptora, sin necesidad de petición previa, se posibilita la transmisión de datos de carácter personal y determinadas informaciones (nombre, apellidos, fecha y lugar de nacimiento, así como la descripción de los hechos que justifican la presunción), en la medida en que sea necesario porque determinados hechos justifiquen la presunción de que las

⁸ Sobre la materia ver, a título de ejemplo, la Decisión 2002/348/JAI y las Resoluciones del Consejo de 6 de diciembre de 2001 y 17 de noviembre de 2003.

personas de que se trate van a cometer delitos según lo dispuesto en la específica normativa comunitaria de lucha antiterrorista⁹.

2.2.2.2. Escolta de seguridad en los vuelos.

Su empleo, de conformidad con la normativa internacional específica¹⁰, en los vuelos de las aeronaves en ella matriculadas, se deja a la decisión de cada Parte Contratante. Los escoltas de seguridad de los vuelos a que se refiere el Tratado serán agentes de policía u otros empleados públicos con la formación correspondiente, encargados de garantizar la seguridad a bordo de las aeronaves. Antes de realizar la escolta de seguridad de un vuelo, el punto de coordinación nacional de la Parte Contratante que envíe la escolta deberá notificar por escrito, con antelación mínima de tres días y contenido mínimo previsto en anexo al Tratado, la utilización de dicha escolta. En caso de peligro inminente, la notificación ulterior se efectuará de manera inmediata antes del aterrizaje.

Las Partes Contratantes concederán a los escoltas de seguridad del vuelo empleados por las otras Partes Contratantes, a petición de dichas Partes Contratantes, una autorización general para llevar armas de servicio, municiones y otros equipos en los vuelos con origen o destino en aeropuertos de las Partes Contratantes. Esta autorización comprenderá tanto la facultad de llevar armas de servicio y municiones a bordo de la aeronave como, con sujeción al apartado 2, en las zonas de seguridad de acceso restringido dentro de un aeropuerto de la Parte Contratante de que se trate. La facultad de llevar armas de servicio y municiones estará sujeta a las siguientes condiciones:

1. La salida de una aeronave en un aeropuerto con armas de servicio y municiones o la estancia en zonas de seguridad de acceso restringido de un aeropuerto de otra Parte Contratante solo podrá efectuarse con el acompañamiento de un representante de la autoridad nacional competente de la Parte Contratante de que se trate.
2. Inmediatamente después de abandonar la aeronave, las armas de servicio y municiones llevadas a bordo se entregarán bajo escolta en un punto de entrega designado por la autoridad nacional competente, donde quedarán depositadas bajo custodia.

⁹ Artículos 1 a 3 de la Decisión Marco n.º 2002/475/JI del Consejo de la Unión Europea, de 13 de junio de 2002, para la lucha contra el terrorismo.

¹⁰ Convenio Internacional de Chicago de 7 de diciembre de 1944, relativo a la aviación civil internacional, y sus anexos, en particular el Anexo n.º 17, así como los demás documentos de aplicación del mismo, y, respecto de las facultades del comandante de a bordo, Convenio de Tokio de 14 de septiembre de 1963, relativo a los delitos y otros actos cometidos a bordo de aeronaves.

2.2.3. Medidas para la lucha contra la migración ilegal.

El Tratado, con este objetivo, prevé dos técnicas de cooperación policial:

2.2.3.1. Envío de asesores en materia de documentos

Estos asesores serán enviados a Estados que se hayan calificado de Estados de origen o tránsito de la migración ilegal. Entre sus funciones, destacan las siguientes:

- Asesoramiento y formación a las representaciones en el extranjero de las Partes Contratantes sobre cuestiones relacionadas con pasaportes y visados, en particular para el reconocimiento de documentos falsos y documentos manipulados.
- Asesoramiento y formación a las empresas de transporte en relación con las obligaciones que les incumben con arreglo a su normativa específica¹¹, así como para reconocer los documentos falsos o manipulados y conocer las disposiciones vigentes en materia de entrada.
- Asesoramiento y formación a las autoridades e instituciones del país anfitrión competentes en materia de control policial en las fronteras.

2.2.3.2. Apoyo en casos de repatriación.

Se prevé apoyo, al amparo de la normativa comunitaria¹², para organizar vuelos conjuntos para la expulsión, desde el territorio de dos o más Estados miembros, de nacionales de terceros países sobre los que hayan recaído resoluciones de expulsión, así como en tránsito a efectos de repatriación por vía aérea. Una Parte Contratante podrá proceder, en la medida en que sea necesario, a la repatriación de una persona a través del territorio de otra Parte Contratante, que decidirá y ejecutará conforme a su derecho interno.

2.2.4. Otras formas de cooperación

2.2.4.1. Patrullas comunes y otras formas de intervención conjunta.

Con el fin de prevenir amenazas para la seguridad y el orden público y para la prevención de los delitos, las autoridades competentes de las Partes Contratantes, podrán organizar patrullas comunes y otras formas de intervención conjunta en las que los funcionarios u otros empleados públicos (en adelante denominados agentes) participen en intervenciones en el territorio de otra Parte Contratante, sin limitarse ya,

¹¹ Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985, relativo a la supresión gradual de los controles en las fronteras comunes, y el Anexo 9 del Convenio de Chicago de 7 de diciembre de 1944 relativo a la aviación civil internacional

¹² Decisión del Consejo de la Unión Europea 2004/573/CE de 29 de abril de 2004 y Directiva 2003/110/CE del Consejo de la Unión Europea, de 25 de noviembre de 2003.

exclusivamente a la zona fronteriza. Cada una de ellas, en calidad de Estado del territorio y con arreglo a su derecho interno, podrá encargar a agentes de otras Partes Contratantes, con el consentimiento de su Estado de origen, el desempeño de facultades soberanas en el marco de intervenciones conjuntas o, cuando el derecho del Estado del territorio lo permita, podrá atribuir a agentes de otras Partes Contratantes el desempeño de sus propias facultades soberanas con arreglo al derecho de su Estado de origen. En todo caso, las facultades soberanas solo podrán ejercerse bajo la dirección y como norma en presencia de agentes del Estado del territorio.

En el Capítulo VI se establecen normas generales sobre el porte de armas de servicio, municiones y equipos permitidos por los agentes de una Parte Contratante que se encuentren en el territorio de otra Parte Contratante en el marco de una intervención conjunta, previendo su uso sólo en caso de legítima defensa, salvo autorización expresa que permita exceder dicho uso.

2.2.4.2. Cruce de frontera.

En caso de urgente necesidad, que define el propio Tratado, los agentes de una Parte Contratante podrán, sin la autorización previa de la otra Parte Contratante, cruzar la frontera común para adoptar en la zona próxima a la frontera dentro del territorio de la otra Parte Contratante, con arreglo al derecho interno del Estado del territorio, las medidas provisionales necesarias para evitar un peligro inminente para la vida o la integridad física de las personas, informando inmediatamente al Estado del territorio, que adoptará, también inmediatamente las medidas necesarias para evitar el peligro de que se trate y hacerse cargo de la situación. Los agentes que realicen la intervención sólo podrán permanecer en el Estado del territorio hasta que el mismo haya adoptado las medidas necesarias para evitar dicho peligro y se atenderán a las instrucciones del Estado del territorio.

Se avanza, en consecuencia, respecto de la “persecución en caliente” prevista en Schengen¹³, limitada a la persecución de delincuentes en el territorio de otro Estado en caso de delito flagrante y siempre que no fuese posible la comunicación inmediata del Estado al que se accedía.

2.2.4.3. Asistencia en caso de grandes eventos, catástrofes y accidentes graves.

Las autoridades competentes de las Partes Contratantes se prestarán apoyo recíproco, con arreglo a su derecho interno, en los eventos masivos y otros

¹³ Art. 41 del Convenio de Aplicación de 19 de junio de 1990 del Acuerdo de Schengen de 14 de junio de 1985.

acontecimientos similares, catástrofes y accidentes graves, a través de una pronta información recíproca, coordinación y asistencia, a petición de la Parte Contratante en cuyo territorio se produzca la situación pertinente, mediante el envío de agentes, especialistas y asesores, y suministro de equipos.

2.2.4.4. Cooperación previa petición.

Con vocación de cláusula de cierre, el Tratado prevé que las autoridades competentes de las Partes Contratantes se prestarán asistencia recíproca previa petición en el marco de sus respectivas competencias y con arreglo a su derecho interno. Además, como refuerzo de técnicas de cooperación fronterizas que se venían llevando a cabo mediante la creación de centros de cooperación policial y aduanera en las propias fronteras, se prevén medidas, en enumeración abierta, consistentes en:

- Averiguación de la identidad del propietario y el usuario y la investigación sobre los conductores de vehículos terrestres, acuáticos y aéreos, en la medida en que no quede ya comprendido en las previsiones sobre consulta automatizada de registros de matriculación.
- Información sobre permisos de conducción, patentes de navegación y habilitaciones semejantes.
- Averiguación de la residencia y del lugar de domicilio.
- Comprobación de los títulos de residencia.
- Averiguación de los titulares de conexiones de teléfono y de otros medios de telecomunicación, en la medida en que sean de acceso público.
- Averiguación de la identidad.
- Investigación sobre la procedencia de objetos, por ejemplo, armas, vehículos de motor y vehículos acuáticos (consultas sobre vías de adquisición).
- Informaciones obrantes en bases de datos policiales y documentos policiales, así como información procedente de recopilaciones de datos oficiales de acceso público.
- Avisos urgentes relativos a armas o explosivos y avisos relativos a falsificaciones de moneda o efectos timbrados.
- Informaciones sobre la ejecución práctica de medidas de observación transfronteriza, persecuciones transfronterizas y entregas controladas.
- Notificación de la disposición de una persona a prestar declaración.

2.2.5. Disposiciones sobre protección de datos de carácter personal.

Aunque resulte discutible y discutida la sinceridad de la preocupación y, sobre todo, la efectividad de la garantía propuesta, desde sus primeros “considerandos”, el

Tratado de Prüm avanza, en una aparente obviedad a la que ya nos referíamos, que las Partes se sitúan “dentro de respeto de los derechos fundamentales” y que son “conscientes en particular de que la transmisión de datos de carácter personal a otra Parte Contratante requiere que en la Parte Contratante receptora se garantice un nivel adecuado de protección de datos”. Sin perjuicio de anunciar otros acuerdos sobre el tema, el Tratado incorpora al Capítulo VII (artículos 33 a 41), disposiciones relativas a la protección de datos, que se aplicarán a los que se transmitan o se hayan transmitido en virtud del Tratado.

La continua remisión en la materia al derecho interno (arts. 2.1, 4.1, 5, 6.1, 10, 14, etc.) ha planteado problemas interpretativos, en cuanto coexistirían, en un doble nivel, normas específicas de protección convencionales, incorporadas al propio Tratado y el Derecho interno, en el que se integrarían tanto normas estatales como comunitarias, que, en aquel momento, se encontraban en fase de desarrollo¹⁴.

2.2.5.1. Definiciones

A los efectos del Tratado, se ofrecen determinadas definiciones auténticas:

- **Tratamiento de datos de carácter personal:** Todo tratamiento o proceso de tratamientos relativo a datos de carácter personal, con o sin ayuda de procedimientos automatizados, tales como la recopilación, almacenamiento, organización, conservación, adaptación o modificación, lectura, consulta, utilización, la comunicación mediante transmisión, difusión o cualquier otra forma de puesta a disposición, la combinación o asociación, así como el bloqueo, cancelación o destrucción de datos; así como la comunicación relativa a la existencia o inexistencia de una concordancia;
- **Consulta automatizada:** Acceso directo a una base de datos automatizada de otra instancia, de tal forma que pueda obtenerse respuesta a la consulta de forma totalmente automática;
- **Marcado:** Inserción de una marca en los datos almacenados de carácter personal sin que con ello se pretenda limitar su tratamiento en el futuro;
- **Bloqueo** se entenderá el marcado de los datos almacenados de carácter personal con el fin de limitar su tratamiento en el futuro.

¹⁴ Propuestas de Decisión Marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal y sobre el intercambio de información en virtud del principio de disponibilidad, COM (2005) 475 y COM (2005) 490, ésta última, como anticipábamos en otro apartado, fallida.

2.2.5.2. Nivel de protección de datos.

Se exige que cada Parte Contratante garantice que su derecho interno ofrezca un nivel de protección de datos equivalente como mínimo al que resulta 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 y el Protocolo Adicional de 8 de noviembre de 2001, y que se atenga a la Recomendación n.º R (87) 15 del Comité de Ministros del Consejo de Europa a los Estados miembros en relación con la utilización policial de datos de carácter personal, de 17 de septiembre de 1987, incluso cuando los datos sean objeto de tratamiento no automatizado.

2.2.5.3. Principio de vinculación a los fines y otros límites de utilización y tratamiento de datos.

- **Uso de datos:** La Parte receptora únicamente podrá utilizar los datos de carácter personal para los fines para los que se transmitieron con arreglo al presente Tratado; el tratamiento de los datos para otros fines requerirá la previa autorización de la Parte titular del fichero y se hará con sujeción al derecho interno de la Parte receptora. La autorización podrá concederse cuando en el derecho interno de la Parte Contratante titular del fichero se admita dicho tratamiento para esos otros fines.
- **Tratamiento de datos:** El tratamiento de los datos transmitidos en consulta automatizada de perfiles ADN y huellas y comparación automatizada de perfiles y dato por la Parte Contratante que realice la consulta o la comparación se encuentra también limitada a determinados fines, fundamentalmente, aquéllos para los que fueron transmitidos (comprobación de coincidencia, preparación de asistencia administrativa o judicial o registro previsto en el propio Tratado).
- También se somete a límites la utilización de datos de vehículos, que se circunscribe, además, al procedimiento que dio lugar a la consulta.
- Los datos de carácter personal transmitidos únicamente podrán ser tratados por las autoridades y tribunales competentes para el desempeño de una función en el marco de los fines previstos en el propio Tratado, exigiéndose, para ulterior comunicación a otras instancias, la autorización previa de la Parte transmitente y sujetándose al derecho interno de la Parte receptora.

2.2.5.4. Garantías de exactitud, actualidad y duración del almacenamiento de los datos.

- **Exactitud y actualidad:** Se impone a las Partes Contratantes la obligación de velar por la exactitud y actualidad de los datos de carácter personal. Si se

comprueba, incluso de oficio, que se han transmitido datos inexactos o que no podían transmitirse, este hecho se comunicará inmediatamente a la Parte o Partes receptoras, que habrán de rectificar o cancelar aquéllos. Los datos cuya exactitud sea rebatida por la persona concernida, pero cuya exactitud o inexactitud no pueda determinarse, deberán ser marcados, si así lo exige la persona concernida, con arreglo al derecho interno de las Partes Contratantes y el marcado solo podrá suprimirse, con arreglo al derecho interno, con el consentimiento de la persona concernida o sobre la base de una resolución del tribunal competente o del órgano independiente competente en materia de control de la protección de datos.

- **Duración del almacenamiento:** Sin perjuicio de la inmediata cancelación de los datos transmitidos o recibidos ilícitamente, también los que lo hayan sido lícitamente están sometidos a límites temporales de almacenamiento, cuando dejen de ser necesarios para los fines que justificaban la transmisión o una vez cumplidos los plazos máximos establecidos en el derecho nacional de la Parte Contratante transmitente para la conservación de los datos, cuando en el momento de la transmisión la autoridad transmitente hubiera informado de dicho plazo máximo a la instancia receptora.
- **Bloqueo:** Es una alternativa a la supresión de datos, acordada con arreglo al derecho interno, cuando existan motivos para creer que la supresión podría afectar a intereses dignos de protección de la persona concernida. Los datos bloqueados solo podrán transmitirse o utilizarse para el fin por el que se prescindió de su supresión.

2.2.5.5. Medidas técnicas y organizativas para garantizar la protección de los datos y su seguridad.

Se impone, con remisión a un acuerdo de ejecución para precisar los pormenores pero con fijación de mínimos, la obligación de conceder una protección eficaz a los datos de carácter personal frente a su destrucción fortuita o no autorizada, su pérdida fortuita, el acceso no autorizado a los mismos, su modificación fortuita o no autorizada y su divulgación no autorizada.

2.2.5.6. Documentación y registro

Las Partes asumen obligaciones de documentación y registro exhaustivo de las consultas y transmisiones, protección frente a usos indebidos y se regula el control jurídico de la transmisión o recepción, que se encarga al órgano independiente competente en materia de control de protección de datos de cada parte.

2.2.5.7. Derechos de las personas concernidas

Se regulan los derechos de las personas concernidas a la información, rectificación, cancelación e indemnización, en su caso, de daños.

EL EQUILIBRIO DE PRÜM	
SEGURIDAD	LIBERTAD
Acceso automatizado a ficheros nacionales (ADN, huellas, vehículos).	Protección de datos de carácter personal
Medidas de prevención de atentados terroristas (información, escoltas de vuelo).	
Medidas de prevención de desórdenes en grandes eventos transfronterizos (deporte, reuniones del Consejo de Europa).	
Medidas contra la migración ilegal.	
Otras medidas (patrullas conjuntas, cruce de fronteras, asesores y centros fronterizos)	

3. La parcial incorporación del Tratado de Prüm al marco jurídico de la Unión Europea

3.1. La Decisión JAI/615/2008

Como sabemos, el Tratado de Prüm, pese a su origen “bastardo” para el europeísmo ortodoxo, nace con “vocación comunitaria”. Desde su primer artículo, se anuncia:

“Como máximo tres años después de la entrada en vigor del presente Tratado, se pondrá en marcha una iniciativa para trasladar las disposiciones del mismo al marco jurídico de la Unión Europea, sobre la base de una valoración de la experiencia

realizada en la ejecución del mismo, previo acuerdo con la Comisión Europea o a propuesta de la Comisión Europea y de conformidad con el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea”.

En una “afortunada coincidencia”, con un vencimiento casi simultáneo, el Programa de La Haya situaba en el 1 de enero de 2008, la fecha a partir de la cual el intercambio transfronterizo de información policial debería regirse por el principio de disponibilidad.

No es extraño que, vista la parcial coincidencia de objetivos a la que también nos hemos referido y aprovechando la Presidencia de Alemania, uno de los cuatro impulsores de Prüm, en la reunión informal de Dresde, los días 15 y 16 de enero de 2007, presentase una **iniciativa¹⁵ destinada a transponer el Tratado de Prüm al marco jurídico de la Unión Europea**. Esta iniciativa fructificaría, no sin recelos¹⁶, pese al apoyo inicial, en el Acuerdo del Consejo de Justicia y Asuntos de Interior de 15 de febrero de 2007, por el que se disponía integrar algunas partes del Tratado de Prüm en el ordenamiento jurídico de la Unión Europea, mediante una decisión basada en el Tercer Pilar, la que sería Decisión JAI/615/2008, de 23 de junio.

En sus **considerandos iniciales**, tras una recapitulación en la que se mencionan, además del Tratado de Prüm, las conclusiones del Consejo Europeo de Tampere, el Programa de La Haya y la ya comentada Decisión Marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, se concluye que el Tratado de Prüm es la respuesta para cumplir con La Haya a tiempo. Igualmente, se parte de la convicción de que, en particular la mejora del intercambio de la información, es objetivo que no puede ser alcanzado satisfactoriamente por los Estados miembros aisladamente, por lo que se adopta la Decisión de acuerdo con los principios de subsidiariedad y proporcionalidad.

En paralelo, se incorpora una declaración de respeto a los derechos fundamentales, en particular el derecho a la intimidad y a la protección de los datos personales, que “debe garantizarse mediante disposiciones especiales de protección de datos adecuadas a las características específicas de las diferentes formas de intercambio de datos. Tales disposiciones de protección de datos deben tener particularmente en cuenta las características propias del acceso transfronterizo en línea a las bases de datos. Dado que, con el acceso en línea, el Estado miembro que gestiona un fichero no puede realizar comprobaciones previas, conviene establecer un sistema que garantice la ejecución de verificaciones a posteriori”. A la hora de incluir

¹⁵ D.O. 28 de marzo de 2007.

disposiciones sobre protección de datos, se tiene presente la ausencia de una Decisión marco sobre protección de datos en el Tercer Pilar, esto es, en materia de cooperación policial y judicial penal, señalándose idéntico estándar mínimo al fijado en el Tratado de Prüm¹⁷.

El **objetivo** de la Decisión, según su artículo 1, es la intensificación de la cooperación transfronteriza en los ámbitos de cooperación policial y judicial en materia penal (Título VI TUE), en particular, del intercambio de información entre las autoridades responsables de la prevención y persecución de delitos. Sus normas se refieren a **cuestiones** ya abordadas por el Tratado de Prüm:

- Condiciones y procedimientos de transferencia automatizada de perfiles de ADN, datos dactiloscópicos y ciertos datos de los registros nacionales de matriculación de vehículos.
- Condiciones de suministro de datos relacionados con acontecimientos importantes que tengan una dimensión transfronteriza, con nueva mención expresa del deporte y de las reuniones del Consejo de Europa.
- Condiciones de suministro de información con el fin de prevenir atentados terroristas.
- Condiciones y procedimientos de intensificación de la cooperación policial transfronteriza a través de otras medidas:
 - Patrullas y otras operaciones conjuntas.
 - Asistencia e caso de concentraciones masivas, catástrofes y accidentes graves.
- Protección de datos.

Los epígrafes, como su desarrollo normativo, son muy similares a los que hemos examinado en el apartado dedicado al Tratado de Prüm. Las diferencias más significativas afectan a la exclusión de la regulación expresa del “cruce de fronteras”, de los “escortas de seguridad de vuelo” y de todo lo relativo a migración ilegal.

¹⁶ Vid el documento de trabajo del Comité de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo de 10 de abril de 2007, Relator Fausto Correia.

¹⁷ Recordemos que este estándar se integraba por el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, y su Protocolo adicional de 8 de noviembre de 2001, tomando en cuenta la Recomendación no R(87) 15, de 17 de septiembre de 1987, del Comité de Ministros a los Estados miembros, dirigida a regular la utilización de datos de carácter personal en el sector de la policía, también cuando los datos no sean tratados de forma automática.

En cuanto a la **articulación normativa** de Tratado y Decisión para las Partes Contratantes del primero, de conformidad con el artículo 35 de la Decisión, se aplicarán las disposiciones pertinentes de la Decisión en lugar de las disposiciones correspondientes contenidas en el Tratado de Prüm. Todas las demás disposiciones del Tratado de Prüm seguirán siendo de aplicación entre las Partes contratantes en dicho Tratado. En relación a otros instrumentos jurídicos, merece ser destacada la declaración según la cual la Decisión no afecta a los acuerdos existentes sobre asistencia judicial o reconocimiento mutuo de las resoluciones judiciales.

3.2. La Decisión JAI/616/2008

Según lo anticipado en el propio Tratado de Prüm y dada la elevada complejidad técnica y jurídica de buena parte de las cuestiones que abordaba aquél, el Tratado fue seguido de un Acuerdo de ejecución administrativo y técnico de 5 de diciembre de 2006. En paralelo y por el mismo motivo, en cumplimiento de lo dispuesto en el 33 de la Decisión 2008/615/JAI, el Consejo, por mayoría cualificada y previa consulta al Parlamento, adoptó las medidas necesarias para la ejecución de aquélla, en la Decisión 2008/615/JAI, de la misma fecha de 23 de junio de 2008, acompañada de un amplio anexo técnico y referida, en particular, como corresponde a su naturaleza, al intercambio automatizado de datos de ADN, datos dactiloscópicos y datos de matriculación de vehículos.

4. El principio de disponibilidad en el Programa de Estocolmo

El devenir del proceso de integración europeo en cuestiones de Justicia e Interior tiene, como hitos fundamentales, la creación del Tercer Pilar en el Tratado de Maastricht, en 1992, la restructuración que realiza el Tratado de Amsterdam, en 1997, al incorporar entre sus objetivos el desarrollo de un Espacio de Libertad, Seguridad y Justicia y el Consejo Extraordinario de Tampere en 1999, en el que se sientan las bases operativas para la concreción de esta área¹⁸ y se afirma que el principio del reconocimiento mutuo, debería convertirse en la piedra angular de la cooperación judicial tanto en materia civil como penal en la Unión.. De este Consejo Extraordinario proviene el primer programa plurianual denominado Programa de Tampere. Si, en su

desarrollo, en condiciones de “impulso y consenso político”, fue innegable el impacto de los atentados del 11-S, el siguiente Programa de La Haya se elaboró, como anticipamos, también en un momento particular, bajo el impacto de los atentados de Madrid de marzo de 2004, que había motivado la Declaración de Bruselas de 25 de marzo de 2004 sobre la Lucha Contra el Terrorismo. Al expirar este segundo Programa, en 2009, la situación que debía abordar el que sería Programa de Estocolmo, para el periodo 2010-2014, era distinta.

Desde el punto de vista jurídico, tras el fracaso del proyecto constitucional europeo, se despejaron las dudas sobre la entrada en vigor del Tratado de Lisboa, el 1 de diciembre de 2009 y, con ello, se abrieron nuevas oportunidades para seguir avanzando en temas de Justicia e Interior, con novedades como la desaparición de los Pilares y consiguiente refundación del sistema legislativo, ampliando las cuestiones excluidas del requisito de unanimidad, el reconocimiento de personalidad jurídica a la Unión Europea o el fortalecimiento de la Comisión, con capacidad para iniciar procesos contra los Estados miembros por incumplimiento de la normativa comunitaria.

Desde el punto de vista sociológico y político, la amenaza del terrorismo internacional se percibe como más lejana y se reduce, paralelamente, la disposición a sufrir recortes de libertades y realizar esfuerzos presupuestarios, en aras de un objetivo que había marcado durante la última década la agenda europea en la materia.

Desde el punto de vista tecnológico, las posibilidades de intromisión en la intimidad y de tratamiento no autorizado de datos personales habían aumentado exponencialmente en una década marcada, entre otras cosas, por el nacimiento y expansión de las redes sociales y la eclosión de las transacciones comerciales online.

La lectura del Programa de Estocolmo¹⁹ revela, desde su título (“Una Europa abierta y segura que sirva y proteja al ciudadano”), que nos encontramos ante un nuevo paradigma. En su adopción, el Consejo Europeo considera que la prioridad para los próximos años será centrarse en los intereses y las necesidades de los ciudadanos. El reto será asegurar el respeto de los derechos y de las libertades fundamentales y la integridad de la persona garantizando al mismo tiempo la seguridad en Europa. En este sentido, “se considera de vital importancia que las

¹⁸ RODRÍGUEZ, J.M y SORROZA BLANCO, A., “El Espacio de Libertad, Seguridad y Justicia y la próxima Presidencia española de 2010. Parte 1ª: la implementación del Tratado de Lisboa y el Programa de Estocolmo”. ARI nº 173/2009, Real Instituto Elcano.

¹⁹ Diario Oficial nº C 115 de 04/05/2010 p. 0001 – 0038.

medidas policiales, por una parte, y las medidas destinadas a salvaguardar los derechos individuales, el Estado de Derecho y las normas de protección internacionales, por otra, vayan unidas en la misma dirección y se refuercen mutuamente”.

En el tema que nos ocupa, merece ser destacado, pues el orden es significativo, que el Programa de Estocolmo sitúa, en primer lugar, entre sus prioridades, el “fomento de la ciudadanía y los derechos fundamentales”, citando expresamente la protección de datos de carácter personal. La referencia a la seguridad (“Una Europa que protege) queda relegada al quinto lugar en el elenco de prioridades.

En cuanto a los instrumentos identificados para cumplir con las prioridades fijadas, al ocuparse de la legislación es evidente el ejercicio de autocrítica al apelar a la aplicación, ejecución y evaluación completas y efectivas de los instrumentos existentes y al señalar que el Consejo Europeo “considera que el desarrollo de la legislación en el ámbito de la libertad, la seguridad y la justicia es impresionante, pero presenta fallos de superposición y cierta falta de coherencia”. Ha llegado el momento de reordenar y, pese a mantenerse la cooperación reforzada, de evitar, en lo posible, situaciones normativas confusas como la generada por el desarrollo paralelo del Tratado de Prüm y el Programa de la Haya.

Ya en el capítulo dedicado a la seguridad, al instar a Consejo y Comisión a diseñar una estrategia de seguridad interior, se introducen las ideas, muy presentes en Prüm, de invitar a “la reflexión sobre un planteamiento anticipatorio y basado en inteligencia”, de “la necesidad de un planteamiento horizontal y transversal para poder abordar crisis complejas o desastres naturales o causados por el hombre”, de “una cooperación rigurosa entre los organismos de la Unión, que incluya una mejora en sus sistemas de intercambio de información” o de una “gestión integrada de las fronteras”.

En otro apartado del mismo capítulo, relativo a la modernización de los instrumentos de trabajo, el Programa se refiere a la gestión del flujo de información, incorporando expresamente la mención del principio de disponibilidad que, se afirma “seguirá dando un importante impulso a esta labor”. Concretando esta afirmación, el Programa insiste en las ideas, recurrentes, de coherencia y consolidación, también en el desarrollo de la gestión y el intercambio de la información, invitando al Consejo y a la Comisión a ejecutar una Estrategia de gestión de la información para la seguridad interior de la UE, que incluya un sistema sólido de protección de datos y, en particular, se invita a la Comisión a evaluar la necesidad de crear un Modelo europeo para el intercambio de información, basado en la evaluación de los instrumentos actualmente existentes, incluidas las ya comentadas Decisiones 2008/615/JAI y 2008/616/JAI del

Consejo y Decisión marco 2006/960/JAI, para determinar si dichos instrumentos funcionan según lo previsto inicialmente y se adecuan a los objetivos de la Estrategia de gestión de la información. Esta Estrategia se define por:

- un desarrollo operativo (un desarrollo del intercambio de información y de sus instrumentos regido por las necesidades en materia de seguridad),
- un sistema sólido de protección de datos acorde con la estrategia de protección de los datos personales a que se refiere el capítulo 2,
- una recopilación de datos bien orientada, tanto a proteger los derechos fundamentales de los ciudadanos como a evitar un exceso de información para las autoridades competentes,
- unos principios rectores de una política de intercambio de información con terceros países a los fines de la seguridad,
- la interoperatividad de los sistemas de tecnologías de la información, velando por una total conformidad con los principios de la protección de datos y la seguridad de los datos al desarrollar dichos sistemas,
- una racionalización de los distintos instrumentos, que incluya la adopción de un plan de actividades para grandes sistemas de tecnologías de la información,
- una coordinación, convergencia y coherencia globales.

El Consejo Europeo pide, además, que se cree un órgano de gestión, con la competencia y la capacidad necesarias para desarrollar técnicamente y gestionar sistemas de gran envergadura de tecnologías de la información en el ámbito de la libertad, la seguridad y la justicia y se avanza iniciativas con vistas a la creación de un sistema de registro de nombres de los pasajeros (PNR) de la Unión.

El Programa de Estocolmo destaca también el principio de disponibilidad, pero incide en su necesaria compatibilidad con la protección de derechos fundamentales.
Reconocimiento de efectos a condenas extranjeras= principio de reconocimiento mutuo

Precisamente otro de los objetivos señalados alude a la movilización de las herramientas tecnológicas necesarias, añadiendo, inmediatamente, “sin dejar de velar por la coherencia con la estrategia de protección de los datos personales”, invitando, en particular, a la mejora del intercambio de información en materia de antecedentes penales, en los términos que examinaremos al final de este tema. Dentro de este mismo objetivo, se insta a la Comisión a:

- Realizar un estudio de viabilidad sobre la necesidad de crear un Sistema Europeo de Fichero Policial (EPRIS), y sobre su valor añadido, y presentar un informe al Consejo al respecto en 2012.

- Reflexionar sobre el modo de extender el uso de las bases de datos de uso policial existentes, respetando plenamente las normas sobre protección de datos, a fin de aprovechar totalmente las nuevas tecnologías para la protección de los ciudadanos.
- Estudiar el mejor modo de facilitar el intercambio de información entre autoridades competentes de los Estados miembros sobre los desplazamientos de delincuentes violentos, incluidos los que acuden a acontecimientos deportivos o a grandes manifestaciones públicas.

Al ocuparse del objetivo de desarrollo de políticas eficaces en materia de seguridad, se insiste en la necesidad de reforzar la eficacia de la cooperación policial europea, siendo evidente el cambio de orientación y prioridades, al señalar que no habría que centrarse únicamente en la lucha contra el terrorismo y la delincuencia organizada, sino también en la expansión de la delincuencia transfronteriza que tiene un impacto significativo en la vida diaria de los ciudadanos de la Unión, rescatando el valor de Europol como eje para el intercambio de información entre las autoridades policiales de los Estados miembros, prestador de servicios y plataforma para los servicios policiales. A tal efecto, se invita a la Comisión y, cuando proceda, al Consejo y a la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad a:

- Estudiar el modo de asegurarse de que Europol reciba información de las autoridades policiales de los Estados miembros.
- Estudiar la forma de intensificar la cooperación policial operativa, por ejemplo en lo que se refiere a la incompatibilidad de los sistemas de comunicaciones y otros equipos.
- Presentar al Consejo y al Parlamento Europeo una propuesta para la adopción de una decisión sobre las modalidades de cooperación, incluido un intercambio de información entre agencias de la Unión, en particular Europol, Eurojust y Frontex, que garantice la protección de los datos y la seguridad,
- Desarrollar una cooperación policial ad hoc para acontecimientos deportivos o grandes manifestaciones públicas.

Más adelante, en relación con la protección contra las formas graves de delincuencia y la delincuencia organizada, se insiste en que este objetivo supondrá la sistematización de los intercambios de información. Destaca la mención expresa, en sede de delincuencia económica y corrupción, del fomento del intercambio de información entre las unidades de información financiera (UIF) en su lucha contra el blanqueo de capitales, con posibilidad de que sus análisis, en el marco del sistema

europeo de gestión de la información, pudieran alimentar una base de datos sobre operaciones sospechosas, por ejemplo en Europol, y de la movilización y coordinación de las fuentes de información para identificar las transacciones en efectivo sospechosas.

A la luz del Programa de Estocolmo, se elaboró un **Plan de acción**, de 25 de noviembre de 2009²⁰ incide en los **aspectos críticos del principio de disponibilidad, cuya mención reitera**. En ejecución de sus previsiones de creación de un régimen general de protección de datos en la Unión Europea, se han elaborado, con la misma fecha de 25 de enero de 2012, la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos²¹ y la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)²², que vendrían a remplazar a la Decisión Marco 2008/977/JAI y a la Directiva 95/46/CE. Igualmente, en la materia que nos ocupa, se está tramitando la Propuesta de Reglamento del Consejo sobre la migración del Sistema de Información de Schengen (SIS 1+) al Sistema de Información de Schengen de segunda generación (SIS II) (refundición)²³.

5. Antecedentes penales

5.1. Introducción

La instauración de un espacio de libertad, seguridad y justicia requiere, entre otras cosas:

- La adecuada circulación, entre las autoridades competentes de los Estados miembros, de la **información relativa a las condenas e inhabilitaciones** de que hayan sido objeto los residentes en el territorio de los Estados miembros, sean nacionales comunitarios o no.
- La posibilidad de **atribuirles efectos fuera del territorio** del Estado miembro

²⁰ Bruselas, 20.4.2010 COM (2010) 171 final.

²¹ Bruselas, 25.1.2012. COM (2012) 10 final.

²² Bruselas 25.1.2012. COM (2012) 11 final.

²³ Bruselas, 30.4.2012. COM(2012) 81 final

que las hubiere pronunciado²⁴.

El primero de estos objetivos, relativo al mero intercambio de información, evoca los postulados del **principio de disponibilidad** que constituye el principal eje de este tema. En cambio, el segundo objetivo, más ambicioso, se sitúa ya en el ámbito del **principio de reconocimiento mutuo** que abordaremos en el Módulo siguiente.

Libre circulación de información sobre condenas ≈ principio de disponibilidad.
Reconocimiento de efectos a condenas extranjeras= principio de reconocimiento mutuo

No se trata, como es sabido, de una inquietud reciente. Son muy numerosos los **convenios** bilaterales que prevén mecanismos de transmisión de información sobre antecedentes penales. Entre los multilaterales, el Convenio Europeo de Asistencia Judicial en Materia Penal de 20 de abril de 1959 (arts. 13 y 22) prevé expresamente, que cada EM debería comunicar la condena al EM del que el condenado es nacional, con carácter anual, manteniendo para estos efectos la comunicación vía autoridad central (frente a la que es regla general de comunicación directa), en art. 6.8 del Convenio 2000. Además, suele entenderse comprendida esta forma de cooperación en el compromiso de prestación de la asistencia más amplia posible que es habitual en los textos convencionales. Por otra parte, algunos convenios internacionales, de modo destacado el Convenio sobre el valor internacional de las sentencias penales del Consejo de Europa (CEVISP); hecho en La Haya el 28 de mayo de 1970, se ocupaban ya de la dimensión más ambiciosa de reconocimiento de efectos a las condenas extranjeras.

En el **Derecho interno** se reconocía, incluso, ocasionalmente, en relación con determinadas modalidades delictivas, efectos a las condenas pronunciadas en el extranjero y este objetivo se encontraba ya explícito en el desarrollo de las conclusiones del Consejo de Tampere en el año 2000.

Y, no obstante, aun contando con estos precedentes, los objetivos de libre circulación y reconocimiento mutuo de condenas en el espacio judicial común, se enfrentaban a serios **obstáculos**.

²⁴ Expresamente se refiere a estos dos objetivos el Libro blanco relativo al intercambio de información sobre condenas penales y al efecto de éstas en la Unión Europea. COM/2005/0010 final, de 25 de enero de 2005.

Respecto de la circulación de información, la primera dificultad venía determinada por las profundas diferencias entre los distintos sistemas nacionales de registro de antecedentes, en cuanto a:

- Autoridad de la que dependen.
- Contenido, ya que algunos recogen sólo las sentencias definitivas, otros se refieren también a personas jurídicas.
- Acceso.
- Reglas de cancelación, en algunos casos automática, en otros a instancia de parte o, incluso, sin posibilidad de cancelación, etc.

En cuanto al intercambio de información sobre sentencias condenatorias, que se ajustaba, básicamente, a los mecanismos del Convenio de 1959, los defectos detectados se referían al incumplimiento de la obligación de envío de la información al EM de nacionalidad del condenado, a la ausencia de identificación de la nacionalidad del condenado, a la insuficiencia de recursos a nivel nacional, a la pérdida o modificación de la información, al “filtrado” de la información por el EM de nacionalidad del condenado, a la ausencia de solicitud de la información, a la sumisión de las escasas solicitudes que efectivamente se cursaban, al lento mecanismo de la comisión rogatoria, sin plazos de cumplimiento y con las dificultades de comprensión, por razón del idioma y de las diferencias de sistema, habituales en la cooperación y, en fin, como un factor más o un resultado de las dificultades anteriores, el juez nacional limitaba, en la práctica totalidad de los casos, su consulta, a los antecedentes nacionales.

Ante la evidencia de tales obstáculos y como preparación para el desarrollo, también en esta materia, del principio de reconocimiento mutuo consagrado en Tampere y que tendría continuidad en el Programa de La Haya, en enero de 2005 se presentó el Libro Blanco relativo al intercambio de información sobre las condenas penales y sus efectos en la Unión Europea²⁵. Pero, a su vez, el Programa de medidas para la puesta en práctica de los fines fijados en Tampere, que representa un verdadero texto programático²⁶ en relación con el principio de reconocimiento mutuo de resoluciones firmes en materia penal, preveía la adopción de uno o varios instrumentos que establecieran el principio en virtud del cual el juez de un Estado miembro debe estar en condiciones de tener en cuenta las resoluciones penales definitivas pronunciadas en los demás para apreciar el pasado penal del delincuente,

²⁵ COM (2005) 10 final, de 25.01.2005.

²⁶ La Comunicación al Consejo y al Parlamento, que lleva fecha de 26 de julio de 2000, condujo a un Programa de medidas (DO C 12, 15.1.2001) para su puesta en práctica presentado por la

para constatar la reincidencia y para determinar la naturaleza de las penas y las modalidades de ejecución que pueden aplicarse.

El primero de estos instrumentos fue la **Decisión 2005/876/JAI del Consejo, de 21 de noviembre de 2005**, relativa a los intercambios de información entre los registros de antecedentes penales, que no modifica, en realidad, el contenido del Convenio de 1959, sino que determina que los antecedentes penales serán solicitados por las autoridades judiciales a su propia autoridad central y ésta los obtendrá directamente, en el caso de corresponder a registros interconectados (Francia, Alemania, España y Bélgica), o los solicitará de los demás, a través de sus autoridades centrales. La autoridad central debía enviar, a intervalos regulares, las condenas de no nacionales al Estado o Estados miembros de nacionalidad y permitía obtener, a los Estados miembros obtener, de conformidad con la legislación nacional, las condenas anteriores pronunciadas contra sus propios nacionales en otros Estados miembros. Entre sus mejoras, cabe destacar el recurso a formularios anexados a la Decisión o el señalamiento de plazo. En 2006 y 2007, la Comisión presentó un amplio paquete legislativo compuesto por tres instrumentos:

- Decisión marco 2008/675/JAI del Consejo por la que se obliga a los Estados miembros a tener en cuenta condenas anteriores con motivo de nuevos procesos penales.
- Decisión marco 2009/315/JAI del Consejo relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales.
- Decisión 2009/316/JAI del Consejo por la que se crea el ECRIS como medio técnico para intercambiar información extraída de los registros de antecedentes penales.

INTERCAMBIO DE INFORMACION ANTECEDENTES		TOMA EN CONSIDERACIÓN CONDENAS
DM 2009/315/JAI (deroga a DM 2005/876/JAI) Fecha límite: 26.3.2012		DM 2008/675/JAI
DM 2009/316/JAI (ECRIS) Fecha límite: 7.4.2012		Fecha límite: 15.8.2010

Comisión donde se incorporan las orientaciones del Consejo JAI de Marsella (de 28 y 29 julio de 2000).

5.2. Decisión Marco 2008/675/JAI del Consejo

Esta DM, de 24 de julio de 2008²⁷, relativa a la consideración de las resoluciones condenatorias entre los Estados miembros de la Unión Europea con motivo de un nuevo proceso penal, tiene por **objetivo** es establecer las condiciones en las cuales se tienen en cuenta, con motivo de un proceso penal contra una persona en un Estado miembro, las condenas anteriores pronunciadas en otros Estados miembros contra la misma persona por hechos diferentes. Debe sustituir a las disposiciones con el mismo objeto del artículo 56 del Convenio Europeo de 28 de mayo de 1970 sobre la validez internacional de las sentencias penales, entre los Estados miembros que son también Partes en ese Convenio.

La **obligación** de toma en consideración se impone a los Estados en la medida en que se tomen en consideración las condenas nacionales anteriores y se atribuyan a aquellas condenas los mismos efectos jurídicos que a las condenas nacionales anteriores, de conformidad con el Derecho nacional. En cuanto a la concreta extensión de esta obligación:

- En sentido positivo, se especifica que se aplicará en la fase previa al proceso penal, durante el propio proceso y en la fase de ejecución de la condena, en particular, en lo que respecta a:
 - la detención provisional;
 - la calificación de la infracción;
 - el tipo y el nivel de la pena impuesta;
 - y la ejecución de la resolución.
- En sentido negativo:
 - Cuando, por motivo de un nuevo proceso, un Estado miembro tenga en consideración las condenas anteriores impuestas en otro Estado miembro, esto no interferirá en las condenas anteriores ni implicará una revocación o revisión de las mismas (a diferencia de lo que sucedería de ser nacional la condena anterior).
 - Si la infracción penal por la que se desarrolla el nuevo proceso se ha cometido antes de que la condena anterior se haya dictado o ejecutado por completo, no se exigirá a los Estados que apliquen su legislación nacional relativa a la imposición de sanciones, si la aplicación de dichas normas a las condenas extranjeras limita al órgano jurisdiccional al imponer una

sanción. No obstante, se garantizará por otros medios que las condenas anteriores se tengan en cuenta en el nuevo proceso.

Pese a que se prevé que la información sobre las condenas se obtendrá “a través de los instrumentos de asistencia judicial aplicables o mediante el intercambio de información extraída de los registros de antecedentes penales”, es lo cierto que las Decisiones 2009/315/JAI y 2009/316/JAI constituyen instrumentos vinculados a la efectividad de esta toma en consideración, lo que puede explicar que la **fecha límite de transposición**, de 15 de agosto de 2010, anterior a la establecida en aquéllas, haya sido ampliamente ignorada.

5.3. Decisión 2009/315/JAI del Consejo

La D.M. 2009/315/JAI, de 26 de febrero de 2009²⁸, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros, deroga la Decisión 2005/876/JAI y complementa, en la materia que constituye su objeto, los Convenios de 1959 y 2000, con sus Protocolos respectivos.

La Decisión tiene por **objeto**:

- Definir el modo en que un Estado miembro de condena debe transmitir información sobre la misma al Estado miembro de nacionalidad del condenado.
- Definir las obligaciones del Estado miembro de nacionalidad del condenado de conservar información sobre condenas.
- Definir los procedimientos que el Estado miembro de nacionalidad del condenado debe seguir cuando responda solicitudes de información sobre sus nacionales.
- Establecer el marco para el desarrollo de un sistema informatizado de intercambio de información.

Se imponen, al **Estado miembro de condena**, las siguientes **obligaciones**:

- Garantizar la inscripción en el registro nacional de antecedentes penales de la nacionalidad o nacionalidades del condenado que no sea nacional propio.
- Comunicar a los restantes Estados miembros las condenas dictadas contra los nacionales de los restantes Estados miembros.
- Comunicar al Estado miembro de nacionalidad del condenado las

²⁷ DO L 220/32, de 15.8.08.

²⁸ DO L 93/23 de 7.4.2009.

posteriores modificaciones o cancelaciones de la información que conste sobre la condena.

- Comunicar al Estado miembro de nacionalidad, a petición de dicho Estado miembro, y en relación con casos particulares, copia de la condena y medidas subsiguientes, o cualquier otra información necesaria para permitirle examinar la necesidad o no de aplicar medidas a nivel nacional.

Por su parte, el **Estado miembro de nacionalidad**, asume las **obligaciones** de:

- Conservar la información recibida sobre cualquiera de sus nacionales con el fin de poder transmitirla posteriormente.
- Modificar o cancelar la información que se le transmitió cuando le sea transmitida una modificación o cancelación de las condiciones de la condena.
- Transmitir, tras cualquier petición, únicamente la información actualizada.

En cuanto al **procedimiento de solicitud** y respuesta, la solicitud se realizará conforme al derecho nacional del Estado solicitante, tanto para que pueda surtir efectos en un procedimiento judicial o para cualquier otro fin, incluso por un particular, pero en este último caso únicamente a condición de que la persona de que se trate sea o haya sido residente o nacional del Estado miembro requirente o del Estado miembro requerido. La solicitud emanada de una autoridad central deberá ajustarse al formulario anexo a la DM.

Respecto de la **respuesta**, la D.M. establece distintos regímenes en función de la razón de la solicitud de información:

- Solicitud realizada en el marco de un procedimiento penal. Se transmitirá información sobre condenas:
 - Pronunciadas en el Estado miembro de nacionalidad que conste en el correspondiente registro.
 - Pronunciadas por terceros Estados miembros y transmitidas con posterioridad al 26 de marzo de 2.012.
 - Transmitidas con anterioridad a tal fecha que se hayan inscrito en el registro de antecedentes penales.
 - Pronunciadas en Estados no miembros que se hayan transmitido e inscrito en el registro de antecedentes penales.

- Solicitud para fines distintos de un procedimiento penal. La respuesta se ajustará al Derecho nacional, en lo que se refiere a las condenas pronunciadas en el Estado miembro de nacionalidad y a las condenas pronunciadas en terceros países que le hayan sido transmitidas y que se hayan inscrito en su registro de antecedentes penales. Respecto a información sobre las condenas pronunciadas en otro Estado miembro, que se hayan transmitido al Estado miembro de nacionalidad, la autoridad central de este último Estado miembro, con arreglo a su Derecho nacional, transmitirá al Estado miembro requirente la información que se haya conservado y la transmitida a dicha autoridad central con anterioridad al 26 de marzo de 2012, y que conste en su registro de antecedentes penales (aunque es posible que el Estado miembro de condena, al transmitir la información al Estado de nacionalidad, haya prohibido la “retransmisión” para fines distintos de un procedimiento penal, en cuyo caso se informará de que la solicitud habrá de dirigirse al Estado de condena).
- Solicitud por tercer país a la autoridad central del Estado miembro de nacionalidad: El Estado miembro podrá responder exclusivamente dentro de los límites establecidos para la transmisión de información a los Estados miembros.

Se establecen distintos plazos, en función del tipo de solicitud, entre la inmediatez o plazo máximo de diez días hábiles si su objeto es surtir efectos en un procedimiento penal u otro fin estatal la respuesta debe ser inmediata, hasta los veinte días hábiles, siempre desde la fecha de la recepción de la solicitud, cuando se realice por petición de una persona.

La información, solicitudes de información y respuestas se realizarán a través de la **Autoridad Central** o Autoridades Centrales de los Estados Miembros

Se reconoce el principio de vinculación a fin de los datos, si bien, excepcionalmente se permite su uso por el Estado miembro requirente para evitar una amenaza inminente y grave para la seguridad pública.

El plazo de transposición de la Decisión expiró el 26 de marzo de 2012.

5.4. Decisión 2009/316/JAI del Consejo La Decisión Marco anterior se complementa por la Decisión 2009/316/JAI del Consejo, de 6 de abril de 2009²⁹ por la que se establece el Sistema Europeo de Información de Antecedentes Penales (ECRIS).

El sistema permitirá la interconexión electrónica de los registros de antecedentes penales, de manera que el intercambio de información entre Estados miembros tenga lugar de forma uniforme y sencilla por vía informática.

Los objetivos de la presente Decisión son los siguientes:

- Establecer la arquitectura general para el intercambio electrónico de información extraída de los registros de antecedentes penales. ECRIS es un sistema descentralizado de tecnología de la información que se basa en las bases de datos de antecedentes penales de los Estados miembros. Consiste en un software de interconexión que permite el intercambio de información entre las bases de datos nacionales y la existencia de una infraestructura de comunicación común, que inicialmente será la red de servicios transeuropeos seguros de telemática entre administraciones (S-TESTA);
- Crear un formato europeo estandarizado de transmisión de información sobre condenas. En este sentido, recoge dos tablas de referencia de categorías de delitos y de categorías de penas, que deberían facilitar la transferencia automática y permitir la comprensión mutua de la información que se transmite mediante un sistema de códigos. Los Estados miembros deberán consultar estas tablas cuando transmitan la información sobre el delito que motivó la condena y la información sobre el contenido de la misma.

El 7 de abril de 2012, los Estados miembros deberían haber tomado las medidas necesarias para ejecutar la Decisión ECRIS.

En cuanto a las perspectivas de futuro, el Plan de Acción del Programa de Estocolmo invitaba a los Estados miembros, a aplicar cuanto antes ECRIS, a la Comisión, a valorar si el establecimiento de una red de antecedentes penales permite evitar la comisión de infracciones penales (por ejemplo, mediante controles de acceso

²⁹ D.O. L 93/33, de 7.4.2009.

a determinados puestos de trabajo, en particular los relacionados con menores), y, si es posible, ampliar el intercambio de información sobre las medidas de supervisión y a proponer, además del ECRIS, un registro de los ciudadanos nacionales de terceros países condenados por órganos jurisdiccionales de los Estados miembros.

Fernando Martínez Pérez

María Poza Cisneros

1 de septiembre de 2012

NIVEL II: PARA SABER MAS

6. El principio de disponibilidad

6.1. Definición

- En la Comunicación de la Comisión al Parlamento Europeo y al Consejo “Reforzar la cooperación policial y aduanera en la Unión Europea”³⁰, de 18 de mayo de 2004, la Comisión hace balance de las medidas y actuaciones que se han adoptado desde el Tratado de Ámsterdam³¹, en el ámbito de la cooperación policial y aduanera, elemento fundamental para mantener un espacio de seguridad. La Comisión apunta, como **factores que obstaculizan la cooperación policial y aduanera**, los siguientes:
 - La naturaleza del trabajo de la Policía.
 - La ausencia de un enfoque estratégico.
 - La proliferación de textos no vinculantes.
 - El procedimiento de decisión del Tercer Pilar.
 - La insuficiente aplicación de los instrumentos jurídicos adoptados por el Consejo.
 - La ausencia de investigación sobre cooperación policial y aduanera.
 - La naturaleza de la cooperación entre la policía y las aduanas.
 - Las bases de datos y los sistemas de comunicación.

La Comisión identificó, como **ámbitos en los que era preciso mejorar**:

- La naturaleza del trabajo de la Policía. El objetivo se fijaba en sensibilizar a las autoridades nacionales desarrollando la confianza mutua, entendiendo indispensable la designación de puntos de contacto nacionales para administrar el intercambio de información, debiendo disponerse por los Estados miembros de un sistema electrónico destinado al intercambio rápido y seguro de información, y hacer uso de las autoridades judiciales de los instrumentos técnicos que faciliten la cooperación.
- El enfoque estratégico. Constatada su ausencia, se reconocía que la norma de la unanimidad en la toma de decisiones retrasaba los progresos deseables.

³⁰ COM 2004/376 final. No publicada en el D.O.

³¹ Entró en vigor el 1 de mayo de 1999.

- La proliferación de textos no vinculantes como problema de la cooperación en el Tercer Pilar. Debían acordarse medidas que fueran efectivamente aplicadas por todos.
- El procedimiento de decisión del Tercer Pilar. La necesidad de decidir por unanimidad y el derecho de iniciativa compartido entre los Estados miembros y la Comisión provocaban que los progresos fueran escasos. Se preveía que la Constitución Europea (fallida, como sabemos) iba a mejorar considerablemente el proceso de decisión.
- La aplicación de los instrumentos jurídicos. Se recordaba que, en el Consejo Europeo de Laeken³², se reafirmó la necesidad de rápida transposición a los derechos nacionales de la Decisiones tomadas por la Unión Europea.
- La investigación sobre la cooperación policial y aduanera. Tras constatarse que la investigación científica en la materia era escasa se proponía dotar medios necesarios para su incremento.
- La naturaleza de la cooperación en la policía y las aduanas. Se manifestaba la necesidad de establecer mayor coordinación y comunicación.
- Las bases de datos y los sistemas de comunicación. Tras citar la existencia de diversas bases de datos y sistemas de comunicación (Sistema de Información Europol, SIS ...) la comisión se preguntaba sobre la interoperabilidad de las diversas, proponiendo el estudio de tres posibles opciones: unificación de los sistemas existentes en uno único, conservarlos independientes y crear nuevos sistemas en caso de necesidad y estudiar y realizar posteriormente la armonización de los formatos de los datos y sus normas de acceso respectivas entre los diversos sistemas.
- En la Comunicación de la Comisión al Consejo y al Parlamento Europeo de 16 de junio de 2.004 “sobre mejora del acceso a la información por parte de las autoridades encargadas de garantizar el cumplimiento de la Ley”³³, se proponía que los Estados miembros adoptasen una **política de información** destinada a:
 - - Hacer accesibles a las autoridades encargadas del cumplimiento de la ley y a las encargadas de la prevención de la delincuencia y el

³² Diciembre de 2.001.

³³ COM 2004/429 final. No publicada en el D.O.

terrorismo los datos necesarios y pertinentes.

- - Estimular la producción y la utilización, en la UE, de información en materia de delincuencia de alta calidad tanto estratégica como operativa
- - Instaurar un clima de confianza entre los servicios competentes, en particular, a través de una protección de los datos personales.

6.2. Transposición del principio

- Sobre los recelos suscitados por el principio de disponibilidad y por el propio Tratado de Prüm, resultan muy ilustrativas las reflexiones y recomendaciones del Supervisor Europeo de Protección de Datos (**SEPD**), en su **Dictamen a la propuesta de Decisión marco del Consejo sobre intercambio de información en virtud del principio de disponibilidad**³⁴. Se señala en él que las dificultades surgen debido al entorno en que debe aplicarse un principio en sí mismo sencillo, **dificultades** que se cifran en:
 - La organización heterogénea de la policía y del poder judicial en los Estados miembros, con controles y equilibrios diferentes.
 - -La inclusión de diversos tipos de información (sensible) (como el ADN o las huellas dactilares).
 - Las diferentes formas de acceso de las autoridades competentes a la información pertinente, incluso dentro de los Estados miembros.
 - La dificultad de garantizar que la información procedente de otro Estado miembro se interprete correctamente debido a las diferencias lingüísticas, de sistemas técnicos (interoperabilidad) y de ordenamientos jurídicos.
 - La necesidad de incluir este principio en el extenso mosaico existente de disposiciones legales sobre intercambio de información policial y judicial entre los distintos países.
- Al referirse a la **iniciativa sueca** que sería, finalmente, la que daría lugar a la DM 2006/960/JAI de 18 de diciembre de 2006, el mismo Dictamen destaca cómo abarca toda la información y la inteligencia, incluso la información e inteligencia que se encuentre en posesión de otras personas distintas de las autoridades policiales y judiciales competentes. Desde el punto de vista de la

³⁴ Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad (COM(2005) 490 final) .Diario Oficial n° C 116 de 17/05/2006 p. 0008 - 0017

protección de datos, se juzga positivo que la propuesta se limite estrictamente al tratamiento de los datos existentes, y que no lleve a la creación de nuevas bases de datos, ni siquiera de "datos índice", si bien se advierte que la falta de "datos índice" no es un elemento positivo por definición. Los datos índice, si se garantizan adecuadamente, pueden facilitar una investigación selectiva y, por eso mismo, menos invasora, de los datos de índole sensible. También puede permitir filtrar mejor las solicitudes, así como una mayor supervisión.

- En relación con el **Tratado de Prüm**, el Dictamen a que nos referimos observa que, en relación con la iniciativa que no prosperó (Propuesta de DM del Consejo, de 12 de octubre de 2005), adopta otro planteamiento sobre la aplicación del principio de disponibilidad. Frente a un planteamiento general que no fija normas específicas para el intercambio de tipos concretos de información, el planteamiento del Tratado de Prüm es gradual o de "campo de datos por campo de datos". Se aplica a tipos específicos de información (ADN, huellas dactilares y datos sobre matriculación de vehículos), y establece la obligación de tener en cuenta la naturaleza específica de los datos. Pero, en un tono abiertamente crítico, el SEPD, realiza las siguientes observaciones sobre el Tratado de Prüm:
 - Respecto de su origen: Advierte, considerándolo, además, obvio, que "no aprueba el proceso que conduce a dicho Tratado, fuera del marco institucional de la Unión Europea, y por lo tanto sin participación sustantiva de la Comisión. Además, ello significa ausencia de control democrático por parte del Parlamento Europeo y ausencia de control judicial por parte del Tribunal de Justicia y como resultado de todo ello menos garantías de que se equilibren de igual modo todos los intereses (públicos)".
 - Respecto de su contenido "invasivo": Estima, también, "obvio que algunos elementos del Tratado de Prüm afectan más a la persona a la que se refieren los datos que la propuesta de una Decisión marco sobre disponibilidad. El Tratado necesariamente conduce al establecimiento de nuevas bases de datos, lo que en sí mismo presenta riesgos para la protección de datos personales. En particular, se critica la imposición de creación de nuevas bases de datos de ADN y una recopilación incrementada de datos de ADN. Además, no resulta claro qué tipo de datos se incluyen en los ficheros de análisis del ADN, y el Tratado no tiene en cuenta la evolución dinámica de los perfiles de ADN.

- Respecto de su planteamiento “ambicioso”. Pese a tratarse, todavía, de un “planteamiento de campo de datos por campo de datos”, se reputa “preferible no establecer un sistema para una diversidad de datos, sino comenzar con un enfoque más cauto que abarque un solo tipo de datos y controlar hasta qué punto el principio de disponibilidad puede efectivamente servir de apoyo a las fuerzas y cuerpos de seguridad, así como vigilar los riesgos específicos para la protección de datos personales. A partir de dichas experiencias, el sistema podría posiblemente ampliarse a otros tipos de datos o modificarse con el fin de ser más efectivo”, lo que resultaría más respetuoso con el principio de proporcionalidad.
- La Exposición de Motivos de la **Propuesta de DM de 12 de octubre de 2005**³⁵, sobre el intercambio de información en virtud del principio de disponibilidad, que no prosperó, hace referencia a su motivación y objetivos. Concretamente, al referirse al contexto general, identifica siete obstáculos principales para que la información esté disponible en toda la UE, con vistas a posibilitar, facilitar o acelerar, la prevención, detección o investigación del delito:
 - Los acuerdos bilaterales y multilaterales entre Estados miembros están geográficamente restringidos o no obligan a los Estados miembros a proporcionar información, con lo que el intercambio de datos depende de factores discrecionales.
 - Las formas actuales de cooperación entre las autoridades policiales y judiciales requieren generalmente la intervención de unidades nacionales de Europol o de puntos de contacto centrales. El intercambio directo de información entre las autoridades sigue siendo la excepción.
 - No existe ningún procedimiento normalizado a escala de la UE para solicitar y obtener información.
 - No existe ningún mecanismo eficiente a escala de la UE que permita saber si existe información disponible y dónde se encuentra.
 - Las diferencias en las condiciones de acceso e intercambio de información, así como en las distinciones entre la cooperación policial, aduanera y judicial impiden un intercambio eficaz de información.

³⁵ COM/2005/0490 final.

- Las diferencias entre los niveles de protección obstaculizan el intercambio de información confidencial.
- No existen normas comunes para el control del uso legal de la información obtenida de otro Estado miembro, y las posibilidades de detectar la fuente y el propósito original de la información son limitadas.

Con la Decisión Marco propuesta, junto con la Decisión Marco también propuesta, sobre protección de datos, se pretendía hacer desaparecer estos obstáculos, hasta el punto de que, con el fin de evitar debilitar el principio de disponibilidad, únicamente cabría negarse a facilitar información por los siguientes motivos:

- Si se comprometiere el resultado de una investigación en curso.
 - Protección de una fuente de información o la integridad física de una persona.
 - Protección de la confidencialidad de la información, en todas las etapas del tratamiento.
 - Protección de los derechos y libertades fundamentales de las personas cuyos datos se tratasen en virtud de la DM.
- La Comunicación de la Comisión al Consejo y al Parlamento Europeo que ofrece un “Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia³⁶” de 20 de julio de 2010 ofrece dos **ejemplos de la utilidad de la denominada Iniciativa o Decisión sueca** para investigar delitos: En 2009 hubo un intento de homicidio en la capital de un Estado miembro. La policía recogió una muestra biológica de un vaso del que había bebido el sospechoso. Tras extraer ADN de esta muestra, los expertos forenses generaron un perfil ADN. La comparación de este perfil con otros perfiles de referencia de la base nacional de datos ADN no dio resultados positivos. Por ello, la fuerza policial que investigaba el caso envió, a través de su punto de contacto Prüm, una solicitud para compararlo con perfiles ADN de referencia de otros Estados miembros a los que se había autorizado a intercambiar esos datos sobre la base de la Decisión Prüm o el Acuerdo Prüm. Esta comparación transfronteriza dio una respuesta positiva. Sobre la base de la Iniciativa sueca, la fuerza policial que investigaba el caso solicitó más datos

³⁶ COM (2010) 385 final, Bruselas, 20.7.2010.

del sospechoso. Su punto de contacto nacional recibió respuestas de otros Estados miembros en 36 horas, lo que permitió a la policía identificar al sospechoso. En 2003 una persona sin identificar violó a una mujer. La policía recogió muestras de la víctima, pero el perfil ADN generado a partir de la muestra no coincidía con ninguno de los perfiles de referencia de la base nacional de datos ADN. Una solicitud de comparación de ADN, enviada por el punto de contacto Prüm a otros Estados miembros a los que se había autorizado a intercambiar perfiles ADN de referencia sobre la base de la Decisión Prüm o el Acuerdo Prüm, tuvo una respuesta positiva. La fuerza policial que investigaba el caso solicitó entonces más información sobre el sospechoso con arreglo a la Iniciativa sueca. Su punto de contacto nacional recibió una respuesta en 8 horas, lo que permitió a la policía identificar al sospechoso.

- La Exposición de Motivos de la **Decisión JAI/615/2008** era explícita al admitir el “aprovechamiento” del material normativo incorporado al Tratado de Prüm para cumplir las exigencias del Programa de la Haya respecto al principio de disponibilidad, al expresarse en estos términos:
 - En el Programa de La Haya, el Consejo Europeo expuso su convicción de que, para conseguir su objetivo, era necesario un planteamiento innovador del intercambio transfronterizo de información entre los servicios de seguridad y, en ese sentido, el Consejo Europeo manifestó que el intercambio de tal información debía cumplir las condiciones aplicables al principio de disponibilidad.
 - La posibilidad de intercambiar con agilidad y eficiencia información exacta es de capital importancia para lograr una cooperación internacional efectiva. Es preciso establecer procedimientos que proporcionen medios rápidos, eficientes y económicos para intercambiar datos.
 - El Tratado de Prüm cumple los requisitos mencionados. Para que todos los Estados miembros cumplan los requisitos sustantivos del Programa de La Haya dentro de los plazos que en él se fijan, es conveniente que el contenido de las partes esenciales del Tratado de Prüm sea aplicable a todos los Estados miembros. La presente Decisión contiene por ello disposiciones basadas en las disposiciones principales del Tratado de Prüm y encaminadas a mejorar el intercambio de información de modo que los Estados miembros se concedan mutuamente derechos de

acceso a sus respectivos ficheros automatizados de análisis de ADN, sistemas automatizados de identificación dactiloscópica y datos de los registros de matriculación de vehículos.

- La intensificación de la cooperación policial y judicial en materia penal debe llevar aparejado el respeto de los derechos fundamentales, en particular el derecho al respeto a la intimidad y a la protección de los datos personales, que debe garantizarse mediante disposiciones especiales de protección de datos adecuadas a las características específicas de las diferentes formas de intercambio de datos.

7. El Tratado de Prüm

7.1. Origen, naturaleza y ámbito de aplicación.

- El Tratado de Amsterdam de 1997 creó la posibilidad formal para algunos Estados miembros de establecer entre ellos una **cooperación reforzada** en el marco de los Tratados. Fue el Consejo Europeo de Feira del 20 de junio de 2000 el que la incorporó formalmente.
 - El Tratado de Niza de 2001, vigente en el momento de gestarse el Tratado de Prüm, facilitó la instauración de una cooperación reforzada: el derecho de veto respecto al establecimiento de una cooperación reforzada de que disponían los Estados miembros desapareció (con excepción de la política exterior), el número de Estados miembros necesarios para iniciar el procedimiento pasó de la mayoría al número fijo de ocho Estados miembros y el campo de aplicación se extendió a la política exterior y de seguridad común (PESC). Las disposiciones sobre el inicio del procedimiento y la posterior participación de un Estado miembro eran diferentes en los tres «pilares». El Tratado de Niza añadió una nueva condición a las ya existentes: este tipo de cooperación debía reforzar el proceso de integración de la Unión y no debe afectar en modo alguno, ni al mercado interior, ni a la cohesión económica y social de la Unión. Además, no podía constituir un obstáculo ni una discriminación a los intercambios entre los Estados miembros, ni provocar distorsiones de competencia entre ellos. Se especificaba el carácter de “último recurso” de este tipo de cooperación, siempre que el Consejo considerase que los objetivos de éstas no

podían alcanzarse, en un plazo razonable, mediante la aplicación de las disposiciones pertinentes de los Tratados. Además, se exigía que estas cooperaciones estuvieran abiertas a todos los Estados miembros en el momento en que se establezcan. También se especificaba que los actos adoptados en el marco de una cooperación reforzada no formarían parte del acervo de la Unión, siendo aplicados en los Estados miembros que participasen, sin impedimento por parte de los demás Estados. Por último, se preveía que el Consejo y la Comisión velarían por la coherencia de las acciones emprendidas en el marco de una cooperación reforzada con las demás políticas y acciones de la Unión.

- Específicamente, el procedimiento de cooperación reforzada era posible tanto en el ámbito del Segundo Pilar, relativo a política exterior y seguridad común, como en el del Tercer Pilar, de cooperación policial y judicial en materia penal. La posibilidad de establecer cooperaciones reforzadas en el ámbito del «segundo pilar», (Título V del Tratado UE) constituye uno de los principales avances del Tratado de Niza en la materia. Pero los procedimientos previstos son diferentes y más rigurosos que en el ámbito del Tercer Pilar y no resulta sencillo siempre, en particular en atención a los contenidos del Tratado de Prüm, delimitar los que pertenecerían a uno u otro Pilar.
- El Tratado de Lisboa facilita el recurso a esta posibilidad que el Tratado constitucional había conservado. El Tratado de Lisboa fija en nueve Estados miembros el umbral mínimo para establecer una cooperación reforzada y permite la aplicación de las «cláusulas pasarela» en las cooperaciones reforzadas, excepto en las decisiones que tengan implicaciones militares o en el ámbito de la Defensa. Estas cláusulas pasarela permiten pasar de la unanimidad a la mayoría cualificada o de un procedimiento legislativo al procedimiento legislativo ordinario. Con carácter general, excluida la materia de política exterior y de seguridad común, los Estados miembros que se propongan establecer una cooperación reforzada dirigirán su solicitud a la Comisión que presentará una propuesta al Consejo. Tras la autorización del Parlamento, el Consejo podrá autorizar la creación de la cooperación reforzada. De forma contraria al procedimiento general, las cooperaciones reforzadas en el ámbito de la PESC no son objeto de propuestas por parte de la Comisión ni de aprobaciones por parte del

Parlamento Europeo. Se decide la creación de tales cooperaciones fundamentalmente en el Consejo. Éste autoriza o no la cooperación reforzada solicitada por los Estados miembros interesados. Se aprueba por unanimidad. Además, la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad deben emitir un dictamen. El Parlamento Europeo solamente es informado de la solicitud. El Tratado de Lisboa ha creado tres tipos de cooperación específica en materia de Defensa y ha facilitado el recurso a las cooperaciones reforzadas en el ámbito de la cooperación judicial en materia penal. El procedimiento de activación se flexibiliza cuando un Estado miembro utiliza «cláusula de freno» para oponerse a la adopción del acto legislativo en este ámbito. En tal caso, se crea una cooperación reforzada de oficio basada en el proyecto legislativo implicado si participan en él al menos nueve Estados miembros. Dicha cláusula, denominada de «acelerador», compensa, de este modo, la cláusula de «freno». Por otra parte, se establecen otras dos cláusulas de acelerador para la creación de una fiscalía europea y la cooperación policial. En ambos casos, para crear una cooperación reforzada, deben participar al menos nueve Estados miembros. Por tanto, dicha cooperación no necesita la propuesta de la Comisión, ni la votación del Consejo.

- El 5 de diciembre de 2006 se firmaba el **Acuerdo Administrativo y Técnico**, en cumplimiento de lo establecido en el artículo 44 del Tratado.
 - El Acuerdo consta de seis secciones. La primera se dedica al objeto y definiciones; la segunda a los perfiles de ADN, pudiendo destacarse que a efectos comparativos las partes harán uso de las normas existentes, como el Conjunto Normalizado de Loci para Europa (ESS) o el Conjunto Normalizado de Loci de INTERPOL (ISSOL) y que el intercambio electrónico de datos relacionados con el ADN entre las Partes se efectuará a través de la red de comunicación TESTA II.
 - En cuanto a la sección tercera, dedicada a los datos dactiloscópicos, las Partes deben establecer un sistema de acceso técnico recíproco a sus “sistemas automatizados nacionales de identificación dactiloscópica” (AFIS) y que el intercambio electrónico de datos dactiloscópicos y datos

relacionados con los mismos entre las Partes se efectuará a través de la red de comunicación TESTA II³⁷

- La sección cuarta se refiere a los datos procedentes de los registros de matriculación de vehículos Para el intercambio electrónico de datos procedentes de los registros de matriculación de vehículos, las Partes utilizarán la red de comunicación TESTA II y una aplicación de software de EUCARIS³⁸ especialmente diseñada para los fines del sistema previsto en el artículo 12 del Tratado.
- **La sección quinta se dedica a la cooperación policial y comprende normas muy concretas sobre intervenciones conjuntas e intervenciones con paso de frontera en supuesto de peligro inminente, figurando en el Anexo D.2 las autoridades a las que se deberá informar inmediatamente, para este último supuesto de colaboración, de conformidad con el artículo 25, apartado 3, del Tratado.**
- **Respecto del primer tipo de colaboración, puede organizarse mediante una declaración de misión, por dos o más Partes, con arreglo al artículo 24 del Tratado. Antes del inicio de la misma, acordarán por escrito o de palabra todo lo relativo a la forma de la intervención, y concretamente:**
 - a) las autoridades competentes de las Partes en la declaración de misión;
 - b) la finalidad concreta de la intervención;
 - c) el Estado del territorio en que se desarrollará la intervención;
 - d) la zona geográfica del Estado del territorio en que se desarrollará la intervención;
 - e) el periodo de tiempo a que se refiere la declaración de misión de la intervención;
 - f) la ayuda concreta que debe proporcionar al Estado del territorio el Estado de origen, que comprenderá agentes u otros funcionarios, material y fondos;**
 - g) los agentes que participarán en la intervención;**
 - h) el agente que estará a cargo de la intervención;

³⁷ Servicios transeuropeos de telemática entre administraciones, gestionados por la Comisión Europea

³⁸ Sistema europeo de información sobre vehículos y permisos

- i) las facultades que podrán ejercer los agentes y otros funcionarios del Estado de origen en el Estado del territorio durante la intervención;
 - j) las armas, municiones y equipos concretos que podrán utilizar los agentes enviados durante la intervención;
 - k) las cuestiones logísticas relacionadas con el transporte, el alojamiento y la seguridad;
 - l) el reparto de los gastos de la intervención conjunta, cuando se aparte de lo dispuesto en el artículo 46 del Tratado;
 - m) cualesquiera otros elementos necesarios.
- Como puede observarse en este Acuerdo no se toman medidas algunas respecto de la inmigración ilegal.

7.2. Contenido

7.2.1. Acceso automatizado a ficheros nacionales

7.2.1.1. Perfiles de ADN

- En esta materia, es preciso insistir, siguiendo el Dictamen del SEPD al que nos hemos referido³⁹, en la **diferencia fundamental entre muestras de ADN y perfiles de ADN**.
 - Las muestras de ADN (a menudo recogidas y almacenadas por autoridades policiales) deberían considerarse como particularmente sensibles, ya que lo más probable es que contengan el conjunto del ADN de una persona. Pueden facilitar información sobre las características genéticas y el estado de salud de una persona, cosa que puede necesitarse para fines totalmente distintos tales como dar consejos médicos a personas o a jóvenes parejas.
 - Los perfiles de ADN, en cambio, contienen únicamente alguna información parcial de ADN extraída de la muestra de ADN: pueden utilizarse para verificar la identidad de una persona, pero en principio no revelan características genéticas de una persona. Con todo, los progresos científicos pueden aumentar la información que puede

³⁹ Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad (COM(2005) 490 final) .Diario Oficial n° C 116 de 17/05/2006 p. 0008 - 0017

revelarse mediante perfiles de ADN: lo que se considera un perfil de ADN "inocente" en un determinado momento, puede revelar en una fase posterior mucha más información de la esperada y necesitada, y en particular información relativa a las características genéticas de una persona. La información que puede revelarse mediante perfiles de ADN debería, por lo tanto, considerarse dinámica.

- El SEPD subraya que **cualquier instrumento jurídico por el que se establezcan intercambios de ADN** debería:
 - Limitar claramente y definir el tipo de información de ADN que podrá intercambiarse (también con respecto a la diferencia fundamental entre muestras de ADN y perfiles de ADN. Establecer unas normas técnicas comunes que tengan como objetivo evitar que las variaciones en el manejo de las bases de datos de ADN de la policía científica en los Estados miembros generen dificultades y resultados incorrectos a la hora de intercambiar datos.
 - Facilitar garantías adecuadas y legalmente obligatorias para evitar que los avances científicos lleven a obtener de los perfiles de ADN datos personales que no sólo sean sensibles, sino también innecesarios para el objetivo para el que fueron recogidos.
- Sobre la eficacia del intercambio de estos datos, al término de la Reunión Informal de Dresde de 15 de enero de 2007, en que fue presentada la iniciativa alemana de transposición del Tratado de Prüm al marco jurídico comunitario, el Ministro alemán de Interior Wolfgang Schäuble, destacó cómo el contraste de las bases de datos de ADN austriaca y alemana, en sólo un mes y medio, desde diciembre de 2006, utilizando el método hit/no hit, encontró 1500 coincidencias de perfiles que figuraban como no identificados en la base alemana, y 1400 respecto de perfiles del mismo tipo en la base austriaca.

7.2.1.2. Datos dactiloscópicos

- Debe tenerse en cuenta la existencia de la base de datos AFIS de Interpol y la europea EURODAC, para solicitantes de asilo.

7.2.1.3. Datos de vehículos

7.2.1.4. Otros datos

Aunque sin mencionarla expresamente, el Tratado suscribe los controvertidos

principios consagrados en la Resolución del Consejo de 29 de abril de 2004 sobre la seguridad de las reuniones del Consejo Europeo y otros acontecimientos similares (2004/C 116/06). La base sobre la cual se permite la transmisión de datos personales se define en la referida Resolución por la existencia de “motivos fundados para creer que [personas o grupos] tienen la intención de entrar en el Estado miembro con el objeto de perturbar el orden público y la seguridad del acontecimiento, o bien de cometer infracciones relacionadas con dicho acontecimiento”. En el art. 14 del Tratado, se hace referencia a la “existencia de condenas firmes o de otras circunstancias [que] justifiquen la presunción de que estas personas van a cometer un delito con motivo del evento o suponen una amenaza para la seguridad y el orden público”. Se ha criticado que, pesa a lo que se pretenda afirmar, el objetivo de esta transmisión de datos personales, basada en “sospechas legitimadas”, que no necesariamente legítimas son personas definidas, más que por un determinado comportamiento, por una ideología política, activistas políticos, en definitiva

7.2.2. Medidas de prevención de atentados terroristas

7.2.2.1. Transmisión de información

- La idea de reunir información con este objeto no es, desde luego, novedosa. Existía un **similar sistema de intercambio de información** con fines de lucha antiterrorista en el contexto del antiguo Grupo de TREVI, que se puso en marcha en 1976 y cuyo ámbito de interés se expandió considerablemente en la década de los 80, para incluir no sólo el terrorismo, sino también la delincuencia organizada, tráfico de drogas e inmigración ilegal. Fue la base para la creación de la Red BdL (bureau de liason), como sistema de transmisión encriptada de información clasificada. La necesidad de contar con un sistema de información rápido y fiable en relación con ataques terroristas alcanzó, por motivos evidentes, una importancia prioritaria a partir de septiembre de 2001. La naturaleza y funcionamiento de esta Red son distintos a los de puntos de contacto nacionales prevista en el Tratado de Prüm, que va más allá, al referirse a intercambios de naturaleza “preventiva”, como tales “bajo sospecha”, en cuanto no está claro, por ejemplo, el modo en que los puntos de contacto nacionales han de acceder al “conocimiento” de que una persona determinada, un sospechoso, va a cometer un delito. Sin embargo, basta este “conocimiento”, esa convicción unilateral de que alguien “puede ser o llegar a ser un terrorista”, para que, conforme al Tratado, las autoridades

puedan transferir datos personales y amplia información prevista en el art. 16, con un enfoque notablemente más amplio que el autorizado por el art 46.1 de Schengen, con más énfasis en el aspecto “preventivo y visionario” confiado a los puntos de contacto nacionales en la lucha contra el terrorismo⁴⁰, invocando la Decisión Marco 2002/475 de 13 de junio de 2002, fraguada superando las dificultades para alcanzar una definición común de terrorismo a través de un concepto amplio que comprende las amenazas de cometer actos terroristas.

- La **designación de puntos de contacto nacionales** a que se refiere el Art. 16.3 del Tratado, que había sido objeto de reiteradas recomendaciones por parte del Consejo y la Comisión, suscita ciertas dudas. En particular, preocupa la ausencia de control democrático en la designación de quienes se califican de verdaderos “oráculos” encargados de pronosticar si un determinado individuo se convertirá o no, en un terrorista y transmitir datos personales e información a otro Estado sobre la base de un pronóstico afirmativo. También se prevé la designación de puntos de contacto y coordinación en relación con los arts. 17 y 18. Pero queda a libertad de los Estados la decisión de qué autoridad o autoridades serán designados, sin descartar la posibilidad de que fuera designado personal de los servicios de inteligencia. Sería posible, incluso, tanto designar puntos de contacto “por materia” o un solo punto de contacto en relación con todos los datos a que se refiere el Tratado. En cambio, el principio de disponibilidad, tal y como es concebido en el Programa de La Haya y su desarrollo apunta a un uso del intercambio de información restringido a las autoridades policiales nacionales y Europol. A título de ejemplo, Bélgica optó por la designación individualizada por materias: el Instituto Nacional de Criminalística y Criminología, dependiente del Ministerio de Justicia, para la transmisión de perfiles de ADN; la Policía Federal, dependiente del Ministerio del Interior, para huellas y otros datos.

7.2.2.2. Escolta de seguridad en los vuelos

- Los mismos autores a quienes seguimos en el apartado anterior han criticado la excesiva discrecionalidad que implica la referencia a “otros empleados públicos con la formación correspondiente” para definir a estos escoltas (“air marshals”).
- EEUU solicitó, tras el 11-S, acompañamiento de este tipo en algunos vuelos procedentes de Europa, originando un amplio debate, motivado por

⁴⁰ BALZACQ et al. “Security and the two level game. The Treaty of Prüm, the EU and the management of threats”

preocupaciones en términos de libertades individuales y en el seno de la Organización Internacional de Aviación Civil, en el que destacó la oposición de los países escandinavos. El Tratado acoge favorablemente esta propuesta, planteando, de este modo, nuevas dudas en relación con el respeto al principio de solidaridad y buena fe, en la medida en que podría establecer un régimen diferenciado para los vuelos procedentes de EEUU.

- Igualmente, ha suscitado preocupación la excepción a la notificación previa por escrito, “en caso de peligro inminente”, no acompañada de una definición de qué haya de entenderse por tal peligro, que podría invocarse bajo la afirmación de que existe (o existía) un “permanente estado de peligro o emergencia” que permitiría la sistemática asignación de estos escoltas a los vuelos, convirtiendo la excepción en norma.

7.2.3. Medidas para la lucha contra la migración ilegal

7.2.3.1. Envío de asesores en materia de documentación

7.2.3.2. Apoyo en casos de repatriación

- Inicialmente, la migración no fue prevista como una política comunitaria. La única mención a la migración recogida en el Tratado de la Comunidad Económica Europea de 25 de marzo de 1.957, se refiere exclusivamente a los trabajadores emigrantes provenientes de los Estados miembros y el objeto de la previsión es asegurarles unas prestaciones sociales adecuadas, que permitan de manera efectiva la libre circulación y el derecho de establecimiento de todo Estado Miembro. La realidad de años posteriores hizo que la inmigración, especialmente la de países no comunitarios, se convirtiera en tema prioritario de los gobiernos de Europa y, como consecuencia, terminase por ser mencionada en un Tratado comunitario, el Acta Única Europea, firmada el 28 de febrero de 1986.
- El Tratado de la Unión Europea es el primer Tratado comunitario en el que se regula de manera propia la inmigración, que ya se considera como un «ámbito de interés común» para la realización de los fines de la Unión, en particular de la libre circulación de personas, y así se recoge en el artículo. K.1, párrafo 3.
- El Tratado de Ámsterdam modifica el de la Unión Europea, entiende las medidas referidas a la inmigración como una parte indisoluble del objetivo de desarrollar la Unión como un espacio de libertad, seguridad y justicia y permite a la Comunidad Europea adoptar medidas en los siguientes campos:

- 1) supresión de controles sobre las personas en el cruce de las fronteras interiores, tanto de ciudadanos de la Unión como de nacionales de terceros países
- 2) el cruce de las fronteras exteriores de la UE
- 3) el asilo y el refugio
- 4) la política de inmigración
- 5) la lucha contra la delincuencia y, como consecuencia, la cooperación policial y judicial en materia penal
- 6) la cooperación judicial en materia civil
- 7) la cooperación a estos efectos entre los servicios de las administraciones de los Estados miembros, y entre dichos servicios y la Comisión.

- El Tratado de Niza prácticamente mantiene la anterior regulación, sin realizar ninguna aportación importante en el campo que tratamos.
- Tras las modificaciones operadas por el Tratado de Lisboa de 13 de diciembre de 2007, la política de inmigración queda encuadrada definitivamente en el espacio de libertad, seguridad y justicia, así “la Unión ofrecerá a sus ciudadanos un espacio de libertad, seguridad y justicia sin fronteras interiores, en el que esté garantizada la libre circulación de personas conjuntamente con medidas adecuadas en materia de control de las fronteras exteriores, asilo, inmigración y de prevención y lucha contra la delincuencia” (artículo 3.2 del actual Tratado de la Unión Europea), regulándose las políticas sobre controles en las fronteras, asilo e inmigración en el Capítulo segundo del Título IV, debiéndose desarrollar una política común sobre “inmigración destinada a garantizar, en todo momento, una gestión eficaz de los flujos migratorios, un trato equitativo de los nacionales de terceros países que residan legalmente en los Estados miembros, así como una prevención de la inmigración ilegal y de la trata de seres humanos y una lucha reforzada contra ambas” (art. 63 bis 1).
- Múltiples son las disposiciones comunitarias sobre la materia, por lo que únicamente a título informativo, y sin olvidar la importancia de las contenidas en el Acervo de Schengen, se señalan a continuación algunas de ellas, que abarcan varios de los campos de la política común:
 - Recomendación del Consejo de 22 de diciembre de 1995 sobre la armonización de los medios de lucha contra la inmigración y el empleo ilegales y sobre la mejora de los medios de control previstos a tal fin

(DO C 5 de 10.1.1996).

- Recomendación del Consejo de 27 de septiembre de 1996 relativa a la lucha contra el empleo ilegal de nacionales de terceros estados(DO C 304 de 14.10.1996).
- Directiva 2001/40/CE del Consejo, de 28 de mayo de 2001, relativa al reconocimiento mutuo de las decisiones en materia de expulsión de nacionales de terceros países (DO L 149 de 2.6.2001).
- Decisión marco del Consejo, de 28 de noviembre de 2002, destinada a reforzar el marco penal para la represión de la ayuda a la entrada, a la circulación y a la estancia irregulares (DO L 328 de 5.12.2002).
- Reglamento (CE) n° 377/2004 del Consejo, de 19 de febrero de 2004, sobre la creación de una red de funcionarios de enlace de inmigración (DO L 64 de 2.3.2004).
- Decisión del Consejo, de 29 de abril de 2004, relativa a la organización de vuelos conjuntos para la expulsión, desde el territorio de dos o más Estados miembros, de nacionales de terceros países sobre los que hayan recaído resoluciones de expulsión (DO L 261 de 6.8.2004).
- Reglamento (CE) n o 562/2006 del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, por el que se establece un Código comunitario de normas para el cruce de personas por las fronteras (Código de fronteras Schengen) (DO L 105 de 13.4.2006).
- Decisión del Consejo, de 26 de abril de 2010, por la que se completa el Código de fronteras Schengen por lo que se refiere a la vigilancia de las fronteras marítimas exteriores en el marco de la cooperación operativa coordinada por la Agencia Europea para la Gestión de la Cooperación Operativa en las Fronteras Exteriores de los Estados miembros de la Unión Europea (DO L 111 de 4.5.2010).

7.2.4. Otras formas de cooperación

- 7.2.4.1. Patrullas comunes y otras formas de intervención conjunta**
- 7.2.4.2. Cruce de frontera**
- 7.2.4.3. Asistencia en caso de grandes eventos, catástrofes y accidentes graves**
- 7.2.4.4. Cooperación previa petición**

7.2.5. Disposiciones sobre protección de datos de carácter personal

- 7.2.5.1. Definiciones**
- 7.2.5.2. Nivel de protección de datos**
- 7.2.5.3. Principio de vinculación a fines y otros límites de utilización y tratamiento de datos**

7.2.5.4. Garantías de exactitud, actualidad y duración del almacenamiento de los datos

7.2.5.5. Documentación y registro

7.2.5.6. Medidas técnicas y organizativas para garantizar la protección de los datos y su seguridad

7.2.5.7.

- Conforme al artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan, debiéndose tratar estos datos de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Asimismo, toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación.
- Como es sabido, el Tratado de la Unión Europea incluyó la colaboración policial entre los Estados miembros en el llamado Tercer Pilar de la Unión Europea, por lo que no existían reglas armonizadas a nivel europeo en materia de protección de datos derivados de esta colaboración, si bien hay un nivel básico común en la legislación de protección de datos de los Estados miembros pues todos ellos pertenecen al Consejo de Europa, basado en el Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) que se aplica a todos los tratamientos de datos de los sectores público y privado, incluso los llevados por las fuerzas y cuerpos de seguridad y al que remite el Tratado de Prüm.
- En 1987 el Consejo de Ministros del Consejo de Europa aprobó la Recomendación (87) 15 por la que se regula el uso de datos personales en el ámbito policial. Esta Recomendación, a decir de ACED FÉLEZ, “se ha convertido en el estándar de facto para la protección de datos en los tratamientos de datos personales llevados a cabo con finalidad de investigación policial a través de su incorporación como requisito mínimo en varios convenios y decisiones de la UE como Schengen, Europol, Sistema de Información Aduanera o Eurojust.”. La Recomendación se articula en torno a ocho principios: control y notificación, recogida de datos, almacenamiento de datos, uso de los datos por parte de la policía, cesiones de datos, publicidad y derechos de las personas, duración del almacenamiento y actualización de los datos, y seguridad de los datos, que establecen los principios básicos por lo que se rige el tratamiento de datos personales en el ámbito policial

- Es política de la Unión Europea, que el intercambio de datos personales en el espacio de libertad, seguridad y justicia, y especialmente en el ámbito de la cooperación policial y judicial, donde se aplica el principio de disponibilidad, y guardando en todo momento el equilibrio entre el derecho a la intimidad y la seguridad, se base en normas claras, pues ello contribuye al aumento de confianza entre las autoridades competentes y garantiza la protección de la información, no bastando los instrumentos jurídicos existentes en el ámbito de la Unión Europea. Así, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1.995 no es de aplicación al tratamiento de datos relacionados con la seguridad pública, la defensa, la seguridad del Estado o las actuaciones del Estado en materia penal.
- Para abordar el problema de la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal en la Unión Europea se dictó, al amparo del principio de subsidiariedad, la Decisión Marco 2008/977/JAI, con el objetivo de proteger los derechos y libertades fundamentales de las personas físicas cuando sus datos personales son utilizados para la prevención, investigación, detección o enjuiciamiento de infracciones penales y ejecución de sanciones penales .
- Ahora bien, debe tenerse en cuenta que varios actos adoptados en virtud del título VI del Tratado de la Unión Europea contienen disposiciones específicas sobre la protección de los datos personales intercambiados, constituyendo en algunos casos un conjunto completo y coherente de normas que regulan estos asuntos con más detalle que la Decisión Marco por lo que ha de entenderse que tales supuestos quedan fuera de su ámbito de aplicación . Igualmente quedan fuera del ámbito de aplicación de la Decisión Marco aquellos supuestos en que las disposiciones existentes por actos concretos dictados al amparo del Título VI del Tratado de la Unión Europea impongan al Estado miembro receptor condiciones más estrictas que las reguladas en la Decisión Marco.
- Así el artículo 28 de la Decisión Marco que tratamos establece que “cuando algún acto, adoptado en virtud del título VI del Tratado de la Unión Europea antes de la fecha de entrada en vigor de la presente Decisión Marco y que regule el intercambio de datos personales entre los Estados miembros o el acceso de unas autoridades designadas de los Estados miembros a sistemas de información establecidos en virtud del Tratado constitutivo de la Comunidad Europea, establezca condiciones específicas respecto de la utilización de dichos datos por el Estado miembro receptor, estas primarán sobre las

disposiciones de la presente Decisión Marco relativas al uso de los datos transmitidos o puestos a disposición por otro Estado miembro”.

- Únicamente podrán recogerse datos con aplicación de los principios de licitud, proporcionalidad y finalidad, y así se establece en el artículo 3 y se tratan en la Decisión Marco, entre otras, las materias de rectificación supresión y bloqueo (de oficio o a instancia del interesado), control de calidad de los datos transmitidos o disponibles, registro y documentación, tratamiento de los datos transmitidos, el ejercicio del derecho de información y acceso a datos los por los interesados, así como el de reparación y la confidencialidad y seguridad del tratamiento de los datos.

8. La parcial incorporación del Tratado de Prüm al marco jurídico de la Unión Europea

8.1. La Decisión JAI/615/2008

8.2. La Decisión JAI/616/2008

Decisión Prüm

Respuestas positivas obtenidas por Alemania en la comparación transfronteriza de perfiles DNA, según el tipo de delito (2009) ¹⁶³					
Respuestas positivas por tipo de delito	Austria	España	Luxemburgo	Países Bajos	Eslovenia
Delitos contra intereses públicos	32	4	0	5	2
Delitos contra la libertad de las personas	9	3	5	2	0
Delitos sexuales	40	22	0	31	4
Delitos contra las personas	49	24	0	15	2
Otros delitos	3 005	712	18	1 105	71

Fuente: Comunicación de la Comisión al Consejo y al Parlamento Europeo que ofrece un “Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia” de 20 de julio de 2010

9. El principio de disponibilidad en el Programa de Estocolmo

- En el Programa de Estocolmo, la enumeración completa de **prioridades** que habrá de tener presente la Unión Europea en su actuación, durante los próximos años, es la siguiente:
 - Fomento de la ciudadanía y los derechos fundamentales Se deberá, por ejemplo, preservar el ejercicio de estos derechos y libertades, en

particular la esfera privada del ciudadano, más allá de las fronteras nacionales, en especial por lo que respecta a la protección de datos de carácter personal.

- Una Europa de la ley y la justicia
- Una Europa que protege
- Acceso a Europa en un mundo globalizado
- Una Europa de la responsabilidad, la solidaridad y colaboración en los ámbitos de la migración y el asilo
- El papel de Europa en un mundo globalizado.
- La dimensión exterior
- En cuanto a los **instrumentos**, se señalan los siguientes:
 - Confianza mutua.
 - Aplicación, ejecución y evaluación completas y efectivas de los instrumentos existentes.
 - Legislación.
 - Aumento de la coherencia.
 - Evaluación.
 - Formación
 - Comunicación
 - Diálogo con la sociedad civil
 - Financiación
 - Plan de acción
- El apartado cuarto, relativo a **seguridad** (“UNA EUROPA QUE PROTEGE) se articula en los siguientes apartados:
 - 4.1. Estrategia de seguridad interior
 - 4.2. Modernización de los instrumentos de trabajo
 - 4.2.1. Forjar una cultura común
 - 4.2.2. Gestionar el flujo de información
 - 4.2.3. Movilizar las herramientas tecnológicas necesarias. En este apartado, el Consejo Europeo invita al Consejo, a la Comisión, al Parlamento Europeo y, en su caso, a los Estados miembros a:
 - elaborar y aplicar políticas que garanticen un elevado nivel de seguridad de las redes y de la información en toda la Unión, y mejorar las medidas destinadas a la protección, la preparación en materia de seguridad y la capacidad de recuperación de las infraestructuras críticas, incluidas las relativas a las Tecnologías

de la Información y la Comunicación (TIC) y los correspondientes servicios,

- promover leyes que garanticen un nivel muy alto de seguridad de las redes y permitan reacciones más rápidas en caso de ciberataques.
- El Consejo Europeo invita también al Consejo y a la Comisión a asegurarse de que las prioridades de la Estrategia de seguridad interior se adapten a las necesidades reales de los usuarios y se centren en la mejora de la interoperatividad. La investigación y el desarrollo en el ámbito de la seguridad deberían ir apoyados por asociaciones entre los sectores público y privado.

4.3. Políticas eficaces

4.3.1. Reforzar la eficacia de la cooperación policial europea

4.3.2. Reforzar la eficacia de la prevención de la delincuencia

4.3.3. Estadísticas

4.4. Protección contra las formas graves de delincuencia y la delincuencia organizada

4.4.1. Lucha contra las formas graves de delincuencia y la delincuencia organizada, priorizando las siguientes tipologías delictivas:

4.4.2. Trata de seres humanos

4.4.3. Explotación sexual de menores y pornografía infantil

4.4.4. Delincuencia cibernética

4.4.5. Delincuencia económica y corrupción

4.4.6. Drogas

4.5. Terrorismo

4.6. Una gestión de catástrofes completa y eficaz por parte de la Unión: reforzar las capacidades de la Unión en materia de prevención, preparación y respuesta frente a todo tipo de catástrofes

- En la línea **crítica** que anticipamos en el Nivel I, respecto del **principio de disponibilidad**, recuerda, expresamente, el **Plan de Acción del Programa de Estocolmo** que:
 - “El principio de disponibilidad podría implicar el riesgo de permitir el intercambio de datos personales que no se han recopilado de modo legítimo respetando la legalidad, por lo que debe fijarse en normas comunes”.

- “Expresa sus dudas con respecto a la facilitación de las actividades operativas que no incluyen una definición europea ni normas comunes a nivel europeo en materia de investigaciones encubiertas, control de los ciudadanos, etc” (acaso con velada referencia al Tratado de Prüm).
- “Considera que, antes de que se prevea una actuación de la Unión Europea en este ámbito, deben establecerse criterios claros para evaluar la proporcionalidad y necesidad de las limitaciones a los derechos fundamentales”
- “Expresa su preocupación por la práctica cada vez más extendida de elaboración de perfiles basada en el uso de técnicas de extracción de datos y de recopilación generalizada de datos pertenecientes a ciudadanos inocentes, con fines preventivos y policiales”
- “Recuerda la importancia de que las acciones encaminadas a hacer cumplir la ley se basen en el respeto de los derechos humanos, desde el principio de la presunción de inocencia al derecho a la intimidad y a la protección de datos”.
- “Destaca la necesidad de fijar unos límites más claros y rigurosos en relación con el intercambio de información entre los Estados miembros, así como en lo que se refiere a la utilización de registros comunes en la Unión Europea; considera que, en caso contrario, el establecimiento de registros de grandes dimensiones a escala de la Unión Europea puede suponer una amenaza para la integridad de las personas y provocar que los registros resulten ineficaces a la vez que aumenten los riesgos de fugas y de corrupción”.
- En cuanto a **propuestas concretas**, en relación con el objeto de estudio, el **Plan de Acción**:
 - Aboga por la mejora del ECRIS.
 - Pide que se revisen 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, el Reglamento (CE) n o 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 por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (3), así como el artículo 13 de la Directiva 95/46/CE del Parlamento Europeo 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 a la libre circulación de estos datos.

- Lamenta que no se haya avanzado en la aplicación del SIS II perfeccionado y del nuevo VIS, e insta a que se eviten nuevos retrasos;
- Destaca la necesidad de desarrollar una administración eficiente, sostenible y segura para los grandes sistemas europeos de tecnologías de la información como los sistemas SIS II, VIS y Eurodac, de forma que se garantice la aplicación plena de todas las normas que regulan dichos sistemas, en función de su finalidad y de los derechos de acceso, así como de las correspondientes medidas de seguridad y protección de datos; destaca, a este respecto, que es esencial que la Unión Europea disponga de un sistema completo y uniforme de normas sobre la protección de datos personales;
- Recuerda que, en determinados ámbitos, la creación de agencias, como la Agencia de los Derechos Fundamentales de la Unión Europea, Eurojust, Europol, Frontex y la Oficina Europea de Apoyo al Asilo, ha sido de gran utilidad para definir un ELSJ; considera que, habida cuenta de que Schengen constituye el núcleo del ELSJ, resulta fundamental y vital crear una agencia europea para la gestión de los sistemas de información sustancial en este ámbito, en particular SIS II, VIS y Eurodac, dado que ésta es la solución más fiable.
- En las iniciativas en trámite tendentes a la implantación de un régimen general de protección de datos en la Unión Europea, se recuerda cómo la piedra angular de la **legislación vigente de la UE en materia de protección de datos**, la Directiva 95/46/CE¹, fue adoptada en 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de datos personales entre los Estados miembros. Se complementó con varios instrumentos que establecen normas específicas sobre protección de datos en el ámbito de la cooperación policial y judicial en materia penal² (antiguo tercer pilar), incluida la Decisión Marco 2008/977/JAI. El Consejo Europeo invitó a la Comisión a evaluar el funcionamiento de los instrumentos de la UE en materia de protección de datos y a presentar, en caso necesario, nuevas iniciativas legislativas y no legislativas. En su resolución sobre el Programa de Estocolmo, el Parlamento Europeo acogió favorablemente un régimen general de protección de datos en la UE y, entre otras cosas, abogó por la revisión de la Decisión Marco. En su Plan de acción por el que se aplica

el programa de Estocolmo, la Comisión subrayó la necesidad de garantizar que el derecho fundamental a la protección de datos de carácter personal se aplique de forma coherente en el contexto de todas las políticas de la UE. La Decisión Marco 2008/977/JAI tiene un ámbito de aplicación limitado, ya que solo se aplica al tratamiento transfronterizo de datos y no a las actividades de tratamiento por parte de las autoridades policiales y judiciales a nivel puramente nacional.

- Aunque no se mencionaba en el Programa de Estocolmo, en enero de 2010, la Presidencia Española presentó una iniciativa de Plataforma de Intercambio de Información Policial, después llamada Plataforma de Intercambio de Información para agentes encargados del cumplimiento de la ley, en términos más amplios (**IXP: Information Exchange Platform for Law Enforcement Authorities**). El propósito era proporcionar un punto de acceso centralizado para autoridades policiales (y judiciales) a cualquier instrumento de intercambio de información policial/judicial a nivel de la UE. La idea fue desarrollada por España y Europol y se sumaron Bélgica, Alemania, Lituania, Hungría, Eslovaquia y la propia Comisión. Aunque todavía en fase muy inicial de desarrollo, sus ejes se sitúan en:
 - Disponer de una página web única, como punto de partida para acceder a productos o servicios relacionados con la cooperación legal internacional, con vistas a una mayor eficiencia en el desarrollo y mantenimiento, más fácil gestión de la protección de datos y la ventaja de una experiencia compartida, en un entorno amable que facilita la identificación de contactos en otros Estados miembros.
 - Abrir el recurso a toda la comunidad europea de autoridades encargadas del cumplimiento de la ley, incluyendo a fuerzas policiales a nivel local, regional o nacional, agentes de aduanas, control de costas y fronteras; a FRONTEX (Agencia Europea para la Gestión de la Cooperación Operativa en las Fronteras Exteriores de los Estados Miembros de la UE; OLAF, Interpol, EMCDDA (Observatorio Europeo de las Drogas y las Toxicomanías OEDT), CEPOL, EuroJust y Europol, jueces, fiscales, servicios penitenciarios, etc.
 - Dar respuesta a las necesidades operativas de la cooperación policial transfronteriza, dando acceso o redirigiendo al usuario a las herramientas, canales e información disponibles, para cubrir áreas como la gestión del conocimiento, la intercomunicación de los usuarios,

el acceso a herramientas específicas para operaciones conjuntas, consultas operativas redirigidas a las bases de datos gestionadas en el marco de justicia, libertad y seguridad, incluso a nivel nacional.

- La Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones de 25 de enero de 2012, sobre “La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI” se ocupa de justificar el nuevo marco jurídico que integrarán la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos y la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), que vendrían a remplazar a la Decisión Marco 2008/977/JAI y a la Directiva 95/46/CE. Señala cómo, “actualmente, el tratamiento de datos por las autoridades policiales y judiciales en materia penal lo regula esencialmente la Decisión Marco 2008/977/JAI, anterior a la entrada en vigor del Tratado de Lisboa. Dado que se trata de una Decisión marco, la Comisión carece de competencia para exigir el cumplimiento de sus disposiciones, lo que ha contribuido a su desigual aplicación. Además, el ámbito de aplicación de la Decisión Marco se limita a las actividades de tratamiento de datos internacionales. Esto significa que el tratamiento de datos personales que no haya sido objeto de intercambio queda actualmente fuera del ámbito de aplicación de las disposiciones de la UE que regulan ese tratamiento y salvaguardan el derecho fundamental a la protección de datos. Además, en algunos casos, esto crea una dificultad práctica a la policía y otras autoridades, para quienes no siempre está claro si el tratamiento de datos ha de ser exclusivamente nacional o internacional, o si los datos nacionales pueden ser objeto de un intercambio internacional subsiguiente. Por consiguiente, el nuevo marco reformado de protección de datos de la UE trata de garantizar un nivel elevado y sistemático de protección de los datos que fomente la confianza mutua entre la policía y las autoridades judiciales de los distintos Estados miembros, contribuyendo con ello a mejorar la libre

circulación de datos y la cooperación efectiva entre la policía y las autoridades judiciales”.

- Con el fin de asegurar un alto nivel de protección de los datos personales en el ámbito de la cooperación policial y judicial en materia penal y de facilitar los intercambios de datos personales entre la policía y las autoridades judiciales de los Estados miembros, la Comisión propone, como parte del paquete de reforma de la protección de datos, una Directiva que:
 - aplique los principios generales de la protección de datos a la cooperación policial y judicial en materia penal, siempre en total respeto de la naturaleza específica de cada uno de estos ámbitos;
 - establezca condiciones y criterios mínimos armonizados para toda posible limitación de las reglas generales; esto se refiere específicamente a los derechos de los ciudadanos a ser informados cuando la policía y las autoridades judiciales manejen sus datos o accedan a ellos; esas limitaciones son necesarias para la prevención, investigación, detección o enjuiciamiento efectivos de los delitos;
 - establezca normas específicas adaptadas a la naturaleza característica de las actividades de los organismos con funciones coercitivas, incluida una distinción entre las distintas categorías de interesados, cuyos derechos pueden variar (como los testigos y los sospechosos).
- En estas nuevas medidas homogeneizadoras del régimen de protección de datos ha de reconocerse el impacto de decisiones del TEDDHH como la **Sentencia de la Gran Sala en el asunto S. y Marper contra el Reino Unido de 4 de diciembre de 2008**, en la que el Estado británico resultó condenado por violación del art. 8 del CEDDHH, en relación con el debido respeto a la vida privada. El asunto trae causa de dos demandas de ciudadanos considerados no culpables por los tribunales, por absolución y archivo, respectivamente, pero cuyas huellas, muestras celulares y perfiles genéticos eran conservados por las autoridades británicas, siendo rechazadas sus reclamaciones, ante la Policía y los tribunales administrativos, de cancelación de datos. El TEDDHH estimó que el carácter general e indiferenciado de la facultad de conservar las huellas dactilares, las muestras biológicas y los perfiles de ADN de las personas sospechosas de haber cometido delitos, pero que no han sido condenadas, no guarda un equilibrio justo entre los intereses públicos y los privados que concurren, y que el Estado demandado superaba con esta normativa y práctica cualquier margen de apreciación aceptable en la

materia, significando la conservación de tales datos en esas circunstancias, una lesión desproporcionada del derecho de los demandantes al respeto de su vida privada, y no puede afirmarse su necesidad en una sociedad democrática.

- Como lectura de cierre, resulta tan desalentadora como “esclarecedora”, la Comunicación de la Comisión al Consejo y al Parlamento Europeo que ofrece un “Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia⁴¹” de 20 de julio de 2010. Uno de sus párrafos, verdadera “sopa de letras”, ofrece una idea bastante aproximada del escenario en el año 2010: La mayoría de los instrumentos analizados tienen una finalidad unitaria: EURODAC pretende mejorar el funcionamiento del sistema de Dublín; la API, mejorar el control fronterizo; la Iniciativa sueca mejorar las investigaciones penales y las operaciones de inteligencia; el Convenio de Nápoles II ayudar a prevenir, detectar, perseguir y castigar el fraude aduanero; el SIA para ayudar a prevenir, investigar y perseguir infracciones graves de las legislaciones nacionales incrementando la efectividad de la cooperación entre las administraciones aduaneras de los Estados miembros; ECRIS, UIF y ORA racionalizar el intercambio transfronterizo de datos en ámbitos concretos; y la Decisión Prüm, la Directiva sobre conservación de datos, el TFTP y el PNR combatir el terrorismo y las formas graves de delincuencia. SIS, SIS II y VIS son las principales excepciones de este modelo: el objetivo original del VIS era facilitar el intercambio transfronterizo de datos sobre visados, pero posteriormente se amplió para prevenir y combatir el terrorismo y las formas graves de delincuencia. SIS y SIS II tienen por finalidad garantizar un elevado nivel de seguridad en el espacio de libertad, seguridad y justicia y facilitar la circulación de personas utilizando la información comunicada a través de este sistema. Con excepción de estos sistemas de información centralizados, la finalidad limitada es un factor central a la hora de diseñar las medidas de gestión de la información a nivel de la UE (...)Otras medidas tratan información personal muy especializada relevante sólo para sus objetivos: los sistemas PNR tratan los detalles de las reservas de vuelos de los pasajeros; FIDE, datos relevantes para la investigación del fraude aduanero; la Directiva sobre conservación de datos, direcciones IP e identificadores de equipos móviles; ECRIS, antecedentes penales; ORA, activos privados y detalles de empresas; las plataformas contra la delincuencia informática, delitos de

⁴¹ COM (2010) 385 final, Bruselas, 20.7.2010.

internet; Europol, vínculos con redes de delincuencia; y el TFTP, datos de mensajería financiera.”

10. Antecedentes penales

10.1. Introducción

- PALOMO DEL ARCO⁴² enumera los principales instrumentos de reconocimiento de condenas penales extranjeras existentes hasta ese momento, cuya insuficiencia, tanto por su irregular implantación en los EEMM, como por su lejanía en cuanto a la consecución de un pleno reconocimiento, justificaría la búsqueda de nuevos mecanismos:
 - El Convenio sobre el valor internacional de las sentencias penales del Consejo de Europa (CEVISP); hecho en La Haya el 28 de mayo de 1970⁴³. “La concepción fundamental que le sirve de base, conforme a su informe explicativo, es la asimilación de una sentencia extranjera (de cualquier Estado Parte) a las que emanan de cualesquiera Tribunales nacionales, con la finalidad expresa, al aceptar la transmisión de la ejecución de las sentencias penales, de favorecer la readaptación social de las personas condenadas. Aunque su contenido, en realidad, se proyecta sobre tres diversas cuestiones: i) la ejecución de la sentencia (arts 2-52); ii) el efecto del principio ne bis in idem (arts. 53-54); y iii) la toma en consideración de sentencias extranjeras en los llamados efectos indirectos (arts. 56-57)”. Entró en vigor con la tercera ratificación, el 26 de julio de 1974. En la actualidad, sólo 22 países lo han ratificado: Albania, Austria, Bélgica, Bulgaria, Chipre, Dinamarca, España, Estonia, Georgia, Islandia, Letonia, Lituania, Moldavia, Montenegro Noruega, Países Bajos, Rumanía, San Marino, Serbia, Suecia, Turquía y Ucrania.
 - Convenio sobre la ejecución de condenas penales extranjeras aprobado en Bruselas, el 13 de noviembre de 1991, en aplicación provisional entre los Países Bajos (incluidas las Antillas holandesas y Aruba) y respectivamente Alemania y Letonia⁴⁴.

⁴² PALOMO DEL ARCO, A. *Antecedentes penales (registro de condenas) en el ámbito europeo*, en *El proceso penal en al Unión Europea: garantías esenciales*, pags. 371-399. Ed. Lex Nova. Valladolid, 2008.

⁴³ Instrumento de ratificación de 2 de septiembre de 1994 (BOE 30.03.96).

⁴⁴ Chipre, España y Portugal también lo han ratificado, pero no han suscrito la cláusula de aplicación provisional.

- Convenio de la UE de 1998 sobre las decisiones de privación del derecho de conducir, adoptado bajo vigencia del Tratado de Maastricht, que posibilita la extensión de la ejecución de las sanciones de privación del derecho de conducir a otros Estados europeos diversos al de la comisión de la infracción y que no ha entrado en vigor.
- Convenio de Aplicación del Acuerdo de Schengen de 14 de junio de 1985 relativo a la supresión gradual de los controles en las fronteras comunes (Schengen, 19 de junio de 1990) contiene en el Capítulo 3 de su Título III normas sobre la aplicación del principio ne bis in idem (artículos 54 a 58), cuya interpretación ha sido objeto de varias sentencias del TJCE, con frecuencia directamente relacionadas con la toma de consideración de las condenas por narcotráfico en otro Estado Miembro de la UE.

10.2. Decisión Marco 2008/675/JAI

- En Francia, el art. 17 de la Ley n° 2010-242 de 10 de marzo de 2010, para la disminución del riesgo de reincidencia y de reforma de distintas normas procesales penales, transpone la Decisión Marco 2008/675. El Código Penal francés preveía ya en su art. 132-16-6 la toma en consideración en sede de reincidencia de las condenas dictadas por la jurisdicción penal de un Estado miembro. El nuevo art. 132-23-1 introduce la norma de equivalencia en la toma en consideración de condenas dictadas por la jurisdicción penal de cualquier otro Estado miembro, en relación con las dictadas en Francia, produciendo unas y otras los mismos efectos jurídicos. Los intérpretes aclaran que, entre esos efectos, se contarían la concesión de la suspensión de ejecución con o sin condiciones, o los criterios de prisión preventiva, que se adopten en lo sucesivo, pero también las revocaciones de suspensión, con o sin condiciones, o de libertad condicional concedidas con anterioridad. Respecto de los efectos de las condenas extranjeras en materia de rehabilitación, esto es, de la cancelación de antecedentes, la entrada en vigor de la reforma, en general prevista para el 1.7.2010, se retrasó hasta el 1.4.2012, pues estos efectos precisaban, a su vez, una reforma más exigente del Registro automatizado de antecedentes, entonces en estudio para la transposición de la Decisión Marco 2009/315/JAI.
- En el Reino Unido, la “Criminal Procedure (Amendment) Law” de 2011 tuvo por objeto la transposición de la Decisión Marco 2008/675.

- El 6 de diciembre de 2011, el Consejo de Estado de Luxemburgo emitió Dictamen sobre el Proyecto de Ley sobre Reincidencia Internacional que significará la transposición al Derecho interno francés de la Decisión Marco 2008/675/JAI. Entre otras cuestiones, se plantea la dificultad de que el juez nacional establezca las necesarias equivalencias, cuando las penas son de distinta naturaleza a las previstas en su Derecho interno, a efectos de garantizar un tratamiento o consideración equivalente de las condenas extranjeras y nacionales anteriores. El proyecto, por otra parte, a diferencia del equivalente francés, al requerir un conocimiento de la condena anterior por las vías tradicionales de asistencia judicial, ignora las Decisiones 2009/315 y 2009/316.

10.3. Decisión Marco 2009/315/JAI

10.4. Decisión 2009/316/JAI

- La reunión del Grupo de Trabajo sobre Cooperación en Materia Penal (expertos ECRIS) de 28 de marzo de 2012 detectó la posibilidad de que los Estados Miembros precisaran **apoyo** para la implementación de ECRIS. Aunque se ha implementado, en plazo, el software comunitario correspondiente (que los Estados miembros pueden optar por usar o no), en la primavera de 2012 se constató un grado variable de implementación técnica y de transposición jurídica en los distintos Estados Miembros, anticipando ya cinco de ellos que no estarían en condiciones de cumplir con la fecha límite de 27.4.2012..
- Parece inminente la publicación de un Manual sobre ECRIS, destinado a autoridades centrales y usuarios finales, entre los que se incluyen jueces, fiscales y policías y la creación de una plataforma central que proporcionaría información, con distintos niveles de acceso.
- Es importante destacar la labor de la Secretaría General del Consejo, a la hora de actualizar los listados anexados a la Decisión, sobre la base de las informaciones que puntualmente deberán transmitir los Estados.

NIVEL III: DOCUMENTACIÓN DE REFERENCIA

11. El principio de disponibilidad

11.1. Definición

- «Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia»

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0184:FIN:ES:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0184:EN:HTML>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0184:FR:HTML>

11.2. Transposición del principio

- DM 2006/960/JAI de 18 de diciembre de 2.006

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:ES:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:EN:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:FR:PDF>

- Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad (COM(2005) 490 final)

<http://eur-law.eu/ES/Dictamen-Supervisor-Europeo-Proteccion-Datos-propuesta-Decision-marco,296571,d>

<http://eur-law.eu/EN/Opinion-European-Data-Protection-Supervisor-Proposal-Council-Framework,296571,d>

<http://eur-law.eu/FR/Opinion-of-the-European-Data-Protection-Supervisor-the,296571,d>

12. El Tratado de Prüm

12.1. Origen, naturaleza y ámbito de aplicación.

- Tratado de Prüm (no hay versión auténtica en inglés)

ES.- <http://www.boe.es/boe/dias/2006/12/25/pdfs/A45524-45534.pdf>

FR.- <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000017865342>

Acuerdo técnico de ejecución del Tratado de Prüm

FR.- <http://textes.droit.org/JORF/2009/07/31/0175/0009/>

12.2. Contenido

12.2.1. Acceso automatizado a ficheros nacionales

- 12.2.1.1. Perfiles de ADN**
- 12.2.1.2. Datos dactiloscópicos**
- 12.2.1.3. Datos de vehículos**
- 12.2.1.4. Otros datos**

- Resolución del Consejo, de 30 de noviembre de 2009 , relativa al intercambio de resultados de análisis de ADN

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:296:0001:01:ES:HTML>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:296:0001:01:EN:HTML>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:296:0001:01:FR:HTML>

12.2.2. Medidas de prevención de atentados terroristas

12.2.2.1. Transmisión de información

12.2.2.2. Escolta de seguridad en los vuelos

- Decisión Marco n.º 2002/475/JAI del Consejo de la Unión Europea, de 13 de junio de 2002, para la lucha contra el terrorismo.

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002F0475:ES:NOT>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002F0475:EN:NOT>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002F0475:FR:NOT>

12.2.3. Medidas para la lucha contra la migración ilegal

12.2.3.1. Envío de asesores en materia de documentación

12.2.3.2. Apoyo en casos de repatriación

- Decisión del Consejo, de 29 de abril de 2004, relativa a la organización de vuelos conjuntos para la expulsión, desde el territorio de dos o más Estados miembros, de nacionales de terceros países sobre los que hayan recaído resoluciones de expulsión 2004/573/CE

<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0573:ES:NOT>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0573:EN:NOT>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0573:FR:NOT>

- Directiva 2003/110/CE del Consejo, de 25 de noviembre de 2003, sobre la asistencia en casos de tránsito a efectos de repatriación o alejamiento por vía aérea

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0110:ES:HTML>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0110:EN:HTML>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0110:FR:HTML>

12.2.4. Otras formas de cooperación

12.2.4.1. Patrullas comunes y otras formas de intervención conjunta

12.2.4.2. Cruce de frontera

12.2.4.3. Asistencia en caso de grandes eventos, catástrofes y accidentes graves

- Resolución del Consejo de 29 de abril de 2004 sobre la seguridad de las reuniones del Consejo Europeo y otros acontecimientos similares (2004/C 116/06).

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:116:0018:0019:ES:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:116:0018:0019:EN:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:116:0018:0019:FR:PDF>

12.2.4.4. Cooperación previa petición

12.2.5. Disposiciones sobre protección de datos de carácter personal

12.2.5.1. Definiciones

12.2.5.2. Nivel de protección de datos

12.2.5.3. Principio de vinculación a fines y otros límites de utilización y tratamiento de datos

12.2.5.4. Garantías de exactitud, actualidad y duración del almacenamiento de los datos

12.2.5.5. Medidas técnicas y organizativas para garantizar la protección de los datos y su seguridad

12.2.5.6. Documentación y registro

- Directiva 95/46/CE del Parlamento Europeo 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 a la libre circulación de estos datos

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML>

- 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

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:es:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:fr:PDF>

13. La parcial incorporación del Tratado de Prüm al marco jurídico de la Unión Europea

13.1. La Decisión JAI/615/2008

<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0615:ES:NOT>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0615:EN:NOT>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0615:FR:NOT>

13.2. La Decisión JAI/616/2008

<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:ES:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:FR:PDF>

14. El principio de disponibilidad en el Programa de Estocolmo

- Programa de Estocolmo

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:es:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:fr:PDF>

- Plan de acción por el que se aplica el Programa de Estocolmo

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:ES:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:FR:PDF>

- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones de 25 de enero de 2012, sobre “La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI”

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:ES:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:FR:PDF>

15. Antecedentes penales

15.1. Introducción

15.2. Decisión Marco 2008/675/JAI

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:220:0032:0034:ES:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:220:0032:0034:EN:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:220:0032:0034:FR:PDF>

15.3. Decisión Marco 2009/315/JAI

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0023:0032:ES:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0023:0032:EN:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0023:0032:FR:PDF>

15.4. Decisión 2009/316/JAI

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0033:0048:ES:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0033:0048:EN:PDF>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0033:0048:FR:PDF>

Anexo: Otros recursos documentales disponibles en inglés o francés

- **BALZACQ, Thierry:** *The Treaty of Prüm and the Principle of Loyalty (art. 10 TEC)*. Centre for European Policy Studies IP/C/LIBE/FWC/2005-08.
- **BALZACQ, T., BIGO D., CARRERA S., GUILD E.:** *Security and the two level game. The Treaty of Prüm, the EU and the Management of Threats*. Centre for European Policy Studies nº234. January 2006.
<http://www.ceps.be/book/security-and-two-level-game-treaty-pr%C3%BCm-eu-and-management-threats>
- **BELLANOVA, Rocco:** *The “Prüm Process:”The Way Forward for EU Police Cooperation and Data Exchange?*
http://vub.academia.edu/RoccoBellanova/Papers/603598/The_Prüm_Process_The_Way_Forward_for_EU_Police_Cooperation_and_Data_Exchange
- **BIGO, D. et al.:** *The principle of information availability*. (hay versión francesa)
<http://www.libertysecurity.org/article1376.html>
- **BUNYAN, Tony:** *The principle of availability*. Statewatch, December 2006.
<http://www.statewatch.org/analyses/no-59-p-of-a-art.pdf>
- **GUILD E., GEYER, F.:** *Getting local. Schengen, Prüm and the dancing procession of Echternach: Three paces forward and two back for EU Police and judicial cooperation in criminal matters*.
<http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=122940>
- **JONES, Chris:** *Implementing the “principle of availability”: The European Criminal Records Information System The European Police Records Index System The Information Exchange Platform for Law Enforcement Authorities*
<http://cadmus.eui.eu/bitstream/handle/1814/6401/LAW-2006-32.pdf?sequence=1>

- **VERVAELE, John A.E.** : *Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?*
<http://www.utrechtlawreview.org/index.php/ulr/article/viewFile/1/1>
Traducción al español actualizada a 2007:
<http://igitur-archive.library.uu.nl/law/2012-0104-200403/Vervaele%20Terrorismo2008.pdf>

- **ZILLER, Jacques**: *Le Traité de Prüm. Une vraie-fausse coopération renforcée dans l'espace de sécurité, de liberté et de justice.*
<http://cadmus.eui.eu/bitstream/handle/1814/6401/LAW-2006-32.pdf?sequence=1>

NIVEL IV: ESPECIFICACIONES PARA ESPAÑA

1. El principio de disponibilidad

1.1. Definición

1.2. Transposición del principio

- La **Ley 31/2010, de 27 de julio, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados Miembros de la Unión Europea⁴⁵**, es la norma de transposición de la Decisión Marco 2006/960/JAI, de 18 de diciembre, tratada en otro nivel del tema. La ley sigue la misma estructura que la decisión Marco, siendo en gran parte de su articulado copia fiel de la misma, pudiendo destacarse las siguientes peculiaridades:
 - Como servicio excluido de su ámbito de aplicación se encuentra el Centro Nacional de Inteligencia (art. 1.3)
 - La lengua a utilizar para la solicitud y el intercambio de información será la aplicable para el canal de comunicación empleado. Se rompe con ello la tónica general de que la comunicación con España debe realizarse en español.
 - Respecto al suministro de información e inteligencia, cuando únicamente se a posible al amparo de una autorización judicial, el órgano judicial competente debe resolver en los breves plazos que se marcan en la Ley para los servicios de seguridad (Disposición Adicional segunda en relación con el artículo 10)
 - Autoridades judiciales competentes para otorgar o denegar, en su caso, la autorización judicial, en los supuestos que sea necesario, son el órgano judicial que conozca del procedimiento judicial abierto en el que se encuentre la información o, en otro caso, los Juzgados Centrales de Instrucción de la Audiencia Nacional.

⁴⁵ Publicada en el BOE de 28 de julio de 2.010, con entrada en vigor al día siguiente de su publicación.

2. El Tratado de Prüm

2.1. Origen, naturaleza y ámbito de aplicación.

- CÁMARA VILLAR se hace eco de las palabras del entonces Presidente del Parlamento Europeo, Josep Borrell, “quien en su Discurso de Bruselas de 17 de octubre de 2005, con motivo de la Conferencia parlamentaria dedicada a la cooperación judicial y policial en Europa, ponía el énfasis en el más necesario control sobre los acuerdos firmados por gobiernos fuera de los Tratados europeos, citando a Prüm y preguntando retóricamente a sus oyentes si habían oído hablar del mismo. «Pues bien –finalizaba su discurso- hasta la fecha, el Parlamento Europeo no ha sido informado. ¿Cuántos Parlamentos de estos países lo han debatido?» Ciertamente, por citar el caso español, resulta en extremo decepcionante acudir a los Diarios de Sesiones de las Cámaras y comprobar cómo en el proceso de ratificación de este Tratado no ha existido el más mínimo debate acerca de sus contenidos”.
- El Instrumento de ratificación se publica en el BOE núm. 307, de 25 de diciembre de 2006. En el mismo se especifica que la entrada en vigor del Tratado para España es el 1 de noviembre de 2006.

2.2. Contenido

2.2.1.1. Acceso automatizado a ficheros nacionales

2.2.1.2. Perfiles de ADN

- En España, como en el resto del mundo, siguiendo en este punto a FIGUEROA NAVARRO, “desde hace más dos décadas, la información obtenida del análisis de muestras biológicas mediante las técnicas de ADN está siendo utilizada en el campo forense como método identificativo”. La primera condena utilizando prueba de este tipo data de 22 de enero de 1988, cuando un tribunal inglés condenó a Colin Pitchfork por asesinato y violación. En la fecha de firma del Tratado de Prüm (2005), la práctica de dicha prueba estaba regulada en España, por la **Ley Orgánica 15/2003**, de 25 de noviembre, que en su disposición final primera modificó los arts. 326 y 363 de la LECrim. y le añadió una nueva disposición adicional tercera, de acuerdo con la cual el Gobierno regularía, mediante Real Decreto, la estructura, composición, organización y funcionamiento de la Comisión Nacional sobre el uso forense del ADN.
- En desarrollo de esta previsión y con mejor técnica legislativa que la anunciada, sería aprobada la **Ley Orgánica 10/2007**, de 8 de octubre, reguladora de la

base de datos policial sobre identificadores obtenidos a partir del ADN. “Con ello, se establece un nuevo marco jurídico que regula, junto a los citados arts. 326 y 363 de la LECrim., la obtención del ADN a partir de muestras biológicas halladas en el lugar del delito, o extraídas de sospechosos, la incorporación de dichos perfiles identificativos a una base de datos única creada al respecto, a fin de que puedan ser utilizados para la investigación de determinados delitos o en los procedimientos de identificación de cadáveres o de averiguación de personas desaparecidas y que permitan el intercambio de dicha información. Asimismo, encomienda a la Comisión Nacional sobre el uso forense del ADN la función de acreditación de todos los laboratorios que realicen análisis de ADN y aporten perfiles genéticos a la citada base de datos policial. El Real Decreto 1977/2008, de 28 de noviembre, vendría a regular la composición y funciones de la **Comisión Nacional para el uso forense del ADN**, además de la anticipada en la Ley, las de elaboración y aprobación de los protocolos técnicos oficiales sobre la obtención, conservación y análisis de las muestras, incluida la determinación de los marcadores homogéneos sobre los que los laboratorios acreditados han de realizar los análisis y la determinación de las condiciones de seguridad en su custodia y la fijación de todas aquellas medidas que garanticen la estricta confidencialidad y reserva de las muestras, los análisis y los datos que se obtengan de los mismos, de conformidad con lo establecido en las leyes.

- Mediante la Orden del Ministerio del Interior 177/2008, de 23 de enero, se crearon “los dos únicos **ficheros policiales** que contienen los datos identificativos obtenidos a partir de los análisis de ADN, tanto en el marco de investigaciones criminales («INT-SAIP») como en los procesos de identificación de cadáveres o de personas desaparecidas (INT-FENIX), siendo el órgano administrativo responsable de los citados ficheros, y de su gestión, el Ministerio del Interior. Igualmente, y en adecuación a lo previsto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, además de la denominación de los citados ficheros, su finalidad y órgano responsable de su gestión, se recogen en esta Orden Ministerial el resto de características exigidas por la mencionada Ley a los ficheros automatizados de las Administraciones Públicas que contienen datos de carácter personal (usos previstos, personas o colectivos sobre los que se pretenden obtener datos de carácter personal o que resulten obligados a suministrarlos, procedimiento de recogida de los datos, estructura básica del fichero y descripción de los datos

de carácter personal incluidos en el mismo, cesiones y transferencias de los datos, órgano administrativo responsable ante el que pueden ejercitarse los derechos de acceso, cancelación y oposición, así como el nivel de medidas de seguridad exigible)”.

- “Respecto a los datos genéticos que pueden ser inscritos en la bases de datos policial que venimos comentando, tanto el Tratado de Prüm como la Ley Orgánica 10/2007 establecen con claridad que tan solo podrán inscribirse en los mencionados ficheros los datos obtenidos a partir del análisis de ADN no codificante, que, si bien permite una identificación absolutamente fiable de la persona, y que es distinto para cada individuo, no permite acceder a otro tipo de información sobre el sujeto, contenida en el ADN codificado, cuyo análisis no queda comprendido en el ámbito material de las normas citadas. Es decir, «los identificadores obtenidos a partir del ADN que proporcionen exclusivamente información genética reveladora de la identidad de la persona y de su sexo», pero en ningún caso los de naturaleza codificante que permiten revelar cualquier otro dato o característica genética”.
- “Ahora bien, el primer paso para obtener el citado perfil genético de una persona, y poder compararlo con otros perfiles de ADN registrados en la base de datos, es contar con una muestra o vestigio biológico para poder realizar el correspondiente análisis de ADN (...) Para ello, y para evitar que la citada prueba pericial de ADN sea tachada de irregular o de ilícita en el proceso penal, es necesario que la obtención de las muestras biológicas de referencia (dubitada e indubitada), y su posterior análisis, se efectúe conforme a las garantías exigidas por nuestra Constitución y leyes procesales, evitando así la vulneración de derechos fundamentales. Ahora bien, el escaso marco normativo que regula la recogida de muestras o vestigios biológicos hallados en el lugar del delito, o la toma de muestras obtenidas directamente de la persona imputada, como ya se indicó anteriormente, y será desarrollado con posterioridad, ha generado múltiples problemas en sede judicial, dictándose sentencias contradictorias, en lo referido a la obtención policial de las muestras (especialmente en las abandonadas por el sospechoso) y en la necesidad o no de contar con la previa autorización judicial. Asimismo, y a falta de un pronunciamiento concreto del Tribunal Constitucional respecto a la posible afectación de derechos fundamentales mediante las intervenciones corporales con la finalidad de obtener perfiles de ADN, la cuestión ha sido abordada por un

Acuerdo del Pleno de la Sala Segunda del Tribunal Supremo. Ante este panorama legislativo y jurisprudencial, la Ley Orgánica reguladora de la base de datos policial de ADN, si bien ha venido a despejar algunas dudas, ha desaprovechado la oportunidad de establecer una regulación más específica y adecuada sobre la materia, que viniera a dar la seguridad jurídica que precisa esta prueba, que se ha convertido en los últimos años en la «prueba estrella» del panorama procesal, no colmando las expectativas que despertaba su aprobación. Así, en lugar de regular la toma de muestras biológicas en su articulado, lo contempla en su Disposición Adicional Tercera, estableciendo que «para la investigación de los delitos enumerados en la letra a) del apartado 1 del art. 3, la policía judicial procederá a la toma de muestras y fluidos del sospechoso, detenido o imputado, así como del lugar del delito. La toma de muestras que requieran inspecciones, reconocimientos o intervenciones corporales, sin consentimiento del afectado, requerirá en todo caso autorización judicial mediante auto motivado, de acuerdo con lo establecido en la LECrim.».

- No obstante, dicho precepto resuelve la cuestión relativa a si para proceder a la recogida de muestras biológicas es siempre necesario contar con la previa autorización judicial. Así, queda claro que tan solo será preceptiva en los casos en que para la toma de las muestras se requiera una intervención corporal (p.e. frotis bucal) y el afectado no preste su consentimiento. Por ello, conforme a esta Disposición Adicional, en sintonía con el citado Acuerdo de la Sala Segunda del Tribunal Supremo de 31 de enero de 2006, será válida una prueba de ADN obtenida de fluidos o restos biológicos arrojados o abandonados por una persona sospechosa de la comisión de un delito (saliva, colillas, prendas de ropa), recogidos por la Policía Judicial sin orden judicial”.
- “No obstante, y a diferencia de otros ordenamientos de nuestro entorno jurídico, en España sigue pendiente una regulación legal pormenorizada de las distintas cuestiones que plantean las intervenciones corporales, y especialmente del uso de la coerción sobre las personas que, en el curso de una investigación penal, y mediando autorización judicial, se negaren a prestar su consentimiento para la práctica de dicha intervención”.
- La Jurisprudencia es clara en lo que se refiere a la **eficacia** probatoria, reconociendo, desde el año 1992, el Tribunal Supremo, un porcentaje de error prácticamente irrelevante, si bien, de modo análogo al razonamiento tradicional en relación con la prueba lofoscópica, “pese a que la pericia de ADN constituye una prueba plena, en lo que respecta a la acreditación de que la persona a la

que se refiere ha estado en contacto con el objeto o víctima en que la muestra ha aparecido, ha de tenerse en cuenta que, como ha puesto de manifiesto la doctrina jurisprudencial de la Sala 2.^a del TS, «cuando la prueba de ADN es la única existente y es factible establecer conclusiones alternativas plausibles, basadas en la incertidumbre o en la indeterminación, el proceso valorativo debe decantarse por una solución absolutoria». La STS 26.7.11, en particular, en relación con el cotejo de muestra con la base de datos policial sobre identificadores genéticos, se reputa innecesario “someter la conclusión así obtenida a un segundo test de fiabilidad, actuando después sobre las muestras de saliva del procesado (...) Es indudable también que el imputado puede rechazar de forma expresa la conclusión pericial sobre su propia identificación genética, cuando ésta se logra a partir de los datos preexistentes en el fichero de ADN creado por la LO 10/2007, 8 de octubre. La posibilidad de que entre el perfil genético que obra en el archivo y los datos personales de identificación exista algún error, es una de las causas imaginables -no la única- de impugnación. Sin embargo, ese desacuerdo, para prosperar, deberá expresarse y hacerse valer en momento procesal hábil. No se trata de enfatizar el significado del principio de preclusión que, en el fondo, no es sino un criterio de ordenación de los actos procesales y, por tanto, de inferior rango axiológico frente a otros valores y principios que convergen en el proceso penal. Lo que se persigue es recordar que la destrucción de la presunción iuris tantum que acompaña a la información genética que ofrece esa base de datos -así lo autorizan la fiabilidad científica de las técnicas de obtención de los perfiles genéticos a partir de muestras ADN y el régimen jurídico de su acceso, rectificación y cancelación, autorizado por la LO 10/2007, 8 de octubre-, sólo podrá ser posible mediante la práctica de otras pruebas de contraste que, por su propia naturaleza, sólo resultarán idóneas durante la instrucción. Sobre esta materia ya nos hemos pronunciado en la STS 685/2010, 7 de julio en un caso idéntico a éste”.

- En suma, el acceso a la base no fue cuestionado en momento procesal hábil, la huella fue obtenida con todas las garantías, en tanto se prestó voluntariamente a tal análisis el procesado, sin que, en consecuencia, fueren necesarias las prevenciones del art. 363 de la Ley de Enjuiciamiento Criminal ; la base o registro ha de considerarse con presunción de exactitud "iuris tantum" en cuanto a los datos que se incorporen a la misma, en tanto no se combatan en el momento procesal hábil para su contraste, y en el caso enjuiciado, la toma de

muestras y obtención y suministro de datos a la base se había realizado en procedimiento diferente a aquel en donde surtían sus efectos, apareciendo la huella como indubitada. A tal efecto, nuestro Acuerdo Plenario de fecha 31 de enero de 2006 permite a la policía judicial la recogida de restos genéticos o muestras abandonadas por el sospechoso, sin necesidad de autorización judicial, que una vez analizadas se han de considerar como indubitadas. La presencia de los peritos en el juicio oral ha sido destacada por la STS 740/2010, de 6 de julio. La colaboración voluntaria del imputado en la toma de muestras de saliva por parte de la policía, ha sido igualmente validada por la STS 634/2010, de 28 de junio, aunque lo preferible fuese la decisión judicial”.

- Mucho más polémica ha resultado la cuestión de la validez constitucional de la prueba, en relación con las circunstancias de la **recogida de la muestra biológica**. “En principio conviene destacar, conforme al criterio de la Sala Segunda del Tribunal Supremo, que «no resulta acorde con la estructura y finalidad del proceso penal la afirmación de que, en ausencia de regulación legal sobre recogida de vestigios, no puedan éstos ser recogidos, analizados y sometidos al dictamen pericial». Se trata, pues, de una prueba pericial legítima, sin perjuicio de que merezca mayor o menor credibilidad en atención a las garantías de su práctica, en ausencia de disposiciones legales que la regulen con suficiencia”.
- Con la escasa base legal proporcionada por los arts. 326 y 363 LECrim. son conocidos los **pronunciamientos contradictorios del Tribunal Supremo** sobre recogida de muestras. “Los hechos similares que dieron lugar a dos pronunciamientos contrarios de la Sala 2ª del Tribunal Supremo son, en resumen, los siguientes: en ambos supuestos los acusados, tras cubrirse el rostro con una capucha para evitar ser reconocidos, procedieron en un caso a la quema de un autobús urbano y en el otro a la explosión de un artefacto situado en un cajero automático de una sucursal bancaria. En la huida, ambos sujetos abandonaron las capuchas empleadas, que fueron recogidas por los agentes de la Ertzaintza al efectuar el acta de inspección ocular del lugar del hecho y sus proximidades. En ambas prendas se encontraron restos biológicos a los que se practicó una prueba de ADN (obteniéndose una muestra dubitada). Con posterioridad, detenidos los sujetos por su implicación en la realización de actos de la llamada «kale borroka», y estando en los calabozos de una Comisaría de la Ertzaintza, en un caso uno arrojó un esputo al suelo de la celda y el otro al salir de la misma. Tales restos biológicos fueron recogidos con un hisopo por

Agentes de la Ertzaintza y enviados a la Policía Científica que, tras el correspondiente análisis de ADN (muestra indubitada), pudieron determinar, en ambos casos, la coincidencia con los perfiles genéticos hallados en las prendas anteriormente descritas. Mediante esta prueba pericial se pudo acreditar la participación de ambos sujetos en cada uno de los anteriores hechos, siendo condenados por la Audiencia Nacional por delitos de daños terroristas. En la primera de las Sentencias (STS 501/2005, de 19 de abril), la Sala de lo Penal del Tribunal Supremo consideró que la prueba indubitada (la del sospechoso) así obtenida había vulnerado el derecho fundamental al proceso con todas las garantías y, en consecuencia, estimó ilícita la citada prueba pericial de ADN, declarando la absolución del procesado, por vulnerarse asimismo su derecho a la presunción de inocencia. Sin embargo, y poco después, la misma Sala (STS 8072/2005, de 14 de octubre) se pronunció en sentido totalmente opuesto, al considerar que, en la obtención de la fuente de prueba (la muestra indubitada), no se vulneró derecho fundamental alguno y, por tanto, la prueba pericial de ADN en este caso fue considerada lícita para fundamentar la sentencia condenatoria. La disparidad de los anteriores pronunciamientos estriba en considerar que, para la toma de dichas muestras, sea necesario o no contar con la previa autorización judicial”.

- La inicial controversia que dividió la Jurisprudencia, acerca del alcance gramatical de los arts. 326, párrafo 3 y 363, párrafo 2 de la LECrim., se ha considerado ya resuelta (SSTS 685/2010, de 7.7 y 22.6.11) y definitivamente clarificada a raíz de la publicación de la LO 10/2007, 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir de ADN. Ya con anterioridad a esta Ley, el Acuerdo del Pleno no jurisdiccional de 31 de enero 2006, había establecido que "la Policía Judicial puede recoger restos genéticos o muestras biológicas abandonadas por el sospechoso sin necesidad de autorización judicial", doctrina incorporada a SSTS 1190/2009, 3 de diciembre, 701/2006, 27 de junio, 949/2006 de octubre y 1267/2006, 20 de diciembre, entre otras
- La STS 25.10.11 destaca “la importancia de que la toma de muestras de saliva u otros fluidos para obtener el perfil genético de cualquier imputado o procesado, se realice con respeto a las garantías impuestas por la intensa injerencia que un acto de esa naturaleza conlleva”, siendo, además, la inmediata consecuencia de la toma de tales muestras su incorporación al registro creado por la LO 10/2007, 8 de octubre. Al respecto y con invocación de

la STS 685/2010, 7 de julio, se distinguen tres supuestos básicos: “a) En primer lugar, cuando se trate de la recogida de huellas, vestigios o restos biológicos abandonados en el lugar del delito, la Policía Judicial, por propia iniciativa, podrá recoger tales signos, describiéndolos y adoptando las prevenciones necesarias para su conservación y puesta a disposición judicial. A la misma conclusión habrá de llegarse respecto de las muestras que pudiendo pertenecer a la víctima se hallaren localizadas en objetos personales del acusado. b) Cuando, por el contrario, se trate de muestras y fluidos cuya obtención requiera un acto de intervención corporal y, por tanto, la colaboración del imputado, el consentimiento de éste actuará como verdadera fuente de legitimación de la injerencia estatal que representa la toma de tales muestras. En estos casos, si el imputado se hallare detenido, ese consentimiento precisará la asistencia letrada. Esta garantía no será exigible, aun detenido, cuando la toma de muestras se obtenga, no a partir de un acto de intervención que reclame el consentimiento del afectado, sino valiéndose de restos o excrecencias abandonadas por el propio imputado; c) en aquellas ocasiones en que la policía no cuente con la colaboración del acusado o éste niegue su consentimiento para la práctica de los actos de inspección, reconocimiento o intervención corporal que resulten precisos para la obtención de las muestras, será indispensable la autorización judicial. Esta resolución habilitante no podrá legitimar la práctica de actos violentos o de compulsión personal, sometida a una reserva legal explícita -hoy por hoy, inexistente- que legitime la intervención, sin que pueda entenderse que la cláusula abierta prevista en el art. 549.1.c) de la LOPJ, colma la exigencia constitucional impuesta para el sacrificio de los derechos afectados”.

- En suma, conviene insistir en la exigencia de asistencia letrada para la obtención de las muestras de saliva u otros fluidos del imputado detenido, cuando éstos sean necesarios para la definición de su perfil genético. Ello no es sino consecuencia del significado constitucional de los derechos de defensa y a un proceso con todas las garantías (arts. 17.3 y 24. 2 CE). Así se desprende, además, de lo previsto en el art. 767 de la LECrim. No es objeto de este recurso determinar las consecuencias de la infracción del derecho de asistencia letrada respecto de los perfiles genéticos que hayan podido incorporarse a la base de datos. El examen de los efectos que esa quiebra podría acarrear, desde el punto de vista probatorio, sólo podrá ser el resultado de la ponderación del caso concreto y de las circunstancias que lo individualicen”.

- El Tribunal Supremo ha elaborado ya un cuerpo de doctrina sobre este tipo de pruebas (perfil genético a través del ADN), integrado, entre otras, por SSTS 5/2011, de 25 de enero, 1027/2010, de 25 de noviembre, 891/2010, de 15 de octubre, 685/2010, de 7 de julio, 740/2010, de 6 de julio, 710/2010, de 15 de junio, 287/2010, de 26 de marzo, 251/2010, de 17 de marzo, 634/2010, de 28 de junio, 123/2010, de 18 de febrero, 398/2010, de 19 de abril, 240/2010, de 24 de marzo, 229/2010, de 15 de marzo, 1190/2009, de 3 de diciembre, 151/2010, de 22 de febrero, y en el ámbito del recurso de revisión, la STS 792/2009, de 16 de julio .
- En particular, respecto del **almacenamiento de datos en ficheros de ADN, la STS 949/2006, de 4 de octubre**, con cita de las SSTS 1311/2005, de 14 de octubre y 179/2006, de 14 de febrero señala que “en materia de investigación policial los análisis se ciñen a desvelar el ADN no codificante con exclusivos fines identificadores, a diferencia de los análisis realizados en el ámbito de la medicina con objetivos investigadores o terapéuticos. Por ello en la Ley Orgánica de Protección de datos de carácter personal, nº 15 de 13 de diciembre de 1999 se prevé un alto nivel de medidas de seguridad, desarrolladas en los reglamentos correspondientes, así como las disposiciones autonómicas, concretamente la orden de 2 de septiembre de 2003 del Departamento de Interior del País Vasco que regula los ficheros automatizados de datos de carácter personal, que sucedió a su equivalente normativo (Orden de 16 de mayo de 1996, del mismo Departamento). Tanto en una disposición como en otra, existen preceptos que garantizan que los datos de carácter personal registrados en los ficheros automatizados sólo serán **utilizados para los fines expresamente previstos** y por personal debidamente autorizado, asegurando en todo caso la confidenciabilidad, seguridad e integridad de los mismos mediante la implantación de medidas conducentes a hacer efectivas las garantías, obligaciones y derechos reconocidos en la Ley Orgánica 15/1999 de 13 de diciembre. En el caso presente no consta en las actuaciones que el proceso posterior de almacenamiento incluya datos más allá de los necesarios para las labores de investigación policial. En todo caso, si el almacenamiento de datos excesivos o innecesarios perjudica o contravine la normativa de la Ley de Protección de Datos será competencia de la Agencia de Protección de Datos investigar el fichero y reducirlo a los términos previstos por la Ley, pero todo ello para nada afecta a la identificación previa realizada con criterios adecuados. Es más, la Orden de 2.9.2003 del Departamento de Interior Vasco, limita su

finalidad a las actividades de policía científica orientadas a relacionar personas con el espacio físico de la infracción penal. En atención a lo expuesto resulta que cualquier temor o recelo de un potencial ataque al "habeas data" está injustificado, sin que por otro lado tales temores tengan que ver con la vulneración del derecho fundamental a la intimidad de la recogida y custodia de muestras si tal cometido se ha realizado con plena acomodación a la normativa vigente. Lo que nunca puede excluirse -recuerda la sentencia citada 179/2006 de 14.2- es que cualquier persona pueda infringir la Ley, en cuyo caso estaría sujeto a las correspondientes sanciones penales o disciplinarias que fueran pertinentes. Pero esa eventualidad en nada afecta a la prueba practicada y a la recogida y conservación de las muestras genéticas, que en ningún aspecto atacan al derecho fundamental contemplado en el art. 18.1 CE”.

- La misma Sentencia citada examina la alegada vulneración del art. 18.4 de la Constitución que “consagra el derecho a la autodeterminación informativa, derecho que debe entenderse como aquel que ostenta toda persona física a la reserva y control de los datos que le conciernen en los distintos ámbitos de la vida, de tal suerte que pueda decidir en todo momento cuando, como y en qué medida esa información sea recogida, almacenada, tratada y en su caso transferida a terceros, así como a ser informado de los datos personales que a estos efectos se encuentren almacenados en ficheros o bases de datos, pudiendo acudir a los mismos con la posibilidad de exigir su identificación, puesta al día o cancelación . No obstante este derecho como todos, tiene excepciones y puede ser limitado por razones de otro interés preponderante. En la Ley de Protección de datos se establece en el art. 6 la exigencia del **consentimiento** inequívoco del afectado, pero en el mismo precepto se establecen **excepciones**. "No será preciso el consentimiento cuando los datos de carácter personal se recogen para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias" y en su art. 2-2c, dispone que el régimen de protección de datos de carácter personal que se establece en dicha ley no será de aplicación a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. De ahí que resulte lógico que cuando la parte solicite certificación de la Agencia General de Protección de Datos sobre la inscripción de los ficheros de la Ertzaintza sobre genética forense, se responda negativamente y que la Orden del Departamento de Interior Vasco de 2.9.2003, omite remitir datos sobre el fichero en cuestión, cuya existencia, características generales y finalidad fueron

oportunamente comunicados a la Agencia de Protección de Datos por el Gobierno Vasco. Y en todo caso -insistimos- el hipotético incumplimiento del registro constituirá una irregularidad administrativa que en modo alguno supone la vulneración de un derecho fundamental que lleve aparejada la nulidad absoluta del análisis practicado. Legislación nacional que se ve reforzada por la Carta de los Derechos Fundamentales de la Unión Europea que en su art. 8 proclama que toda persona tiene derecho a la protección de los datos de carácter personal y que solo podrán ser recogidos mediante su consentimiento o en virtud de otro fundamento legítimo previsto por la Ley, y por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, cuyo art. 8 señala que la salvaguardia de la intimidad permite la injerencia prevista por la Ley, cuando se trate de medidas aceptables en una sociedad democrática para la prevención del delito”.

- Si el almacenamiento de datos excesivos o innecesarios perjudica o contraviene la normativa de Protección de Datos, será competencia de la Agencia de Protección de Datos investigar el fichero y reducirlo a los términos previstos por la Ley. La Ley Orgánica 10/2007, reguladora de la base de datos policial de ADN, destaca, en su Preámbulo, «el carácter sensible que dichos datos tienen y el importante grado de protección con que, naturalmente deben contar» y establece específicas garantías en aras de preservar el derecho a la intimidad que sistematiza FIGUEROA NAVARRO en las siguientes:
- La inscripción en los citados ficheros se limita a «los identificadores obtenidos a partir del ADN que proporcionen exclusivamente información genética relativa a la identidad de la persona y de su sexo».
- Los datos que se inscribirán son «los identificativos extraídos a partir del ADN de muestras o fluidos que hubieran sido hallados u obtenidos a partir del análisis de las muestras biológicas del sospechoso, detenido o imputado, cuando se trate de delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada, debiendo entenderse incluida, en todo caso, en el término delincuencia organizada la recogida en el art. 282 bis, apartado 4 de la Ley de Enjuiciamiento Criminal en relación con los delitos enumerados».
- La inscripción en la base de datos policial de los anteriores datos identificadores obtenidos a partir del ADN «no precisará del consentimiento del afectado, el

cual será informado por escrito de todos los derechos que le asisten respecto a la inclusión en dicha base, quedando constancia de ello en el procedimiento».

- El uso de los datos contenidos en el presente fichero se limita a «las Unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado, entendiendo por tales las Unidades respectivas de la Policía y de la Guardia Civil en el ejercicio de sus funciones» y a «las Autoridades Judiciales y Fiscales, en la investigación de los delitos previstos en el art. 3 de esta Ley».
- Podrán cederse los citados datos a «las Autoridades Judiciales, Fiscales o Policías de terceros países de acuerdo con lo previsto en los Convenios internacionales ratificados por España y que estén vigentes». Asimismo, a las «Policías Autonómicas y al Centro Nacional de Inteligencia».
- Finalmente, y de acuerdo con lo establecido en la Ley Orgánica de Protección de Datos, la Ley Orgánica 10/2007 contiene las previsiones correspondientes respecto a la cancelación, rectificación y acceso a los datos (art. 9), estableciendo que «todos los ficheros que integran la base de datos objeto de esta ley están sometidos al nivel de seguridad alto» (art. 8).
- En el estudio realizado para valorar el impacto de la STEDDHH en el caso S. y Marper contra el Reino Unido, en relación con la regulación y práctica procesal española, HOYOS avanza determinadas conclusiones. En cuanto a la exigencia de legalidad, pese a encontrarse garantizada en Derecho español, se destacan lagunas como la muy importante relativa a la posibilidad de obtención coactiva de una muestra orgánica en caso de negativa del sospechoso a prestarla, concreción del concepto "delito grave", consentimiento y tratamiento del menor sospechoso, presupuestos de la destrucción-conservación de las muestras corporales o vestigios o designación de la autoridad ante la que se instará la cancelación o certificación, entre otros aspectos. Por otro lado, se valora "muy positivamente que en España, en la línea de la normativa comunitaria más reciente, y ya antes en el referido Tratado de Prüm, sólo se pueda integrar en los archivos policiales el denominado ADN no codificante. No obstante, esta garantía de que la injerencia en la vida privada o en la intimidad del sospechoso será la mínima imprescindible para los fines legítimos, podría verse desvirtuada por la conservación sin presupuestos ni límites claros de vestigios o muestras corporales para eventuales análisis o contraanálisis ulteriores –art. 5.1 LO 10/2007". En cuanto al exigible grado de necesidad de la injerencia, si bien sólo accederán al fichero las personas sospechosas de comisión de delito (al margen de incorporación voluntaria de datos) se cuestiona el grado de

sospecha exigible como presupuesto, señalando que “la proporcionalidad entre los medios empleados y los fines perseguidos –investigación y prevención de hechos delictivos– sólo se respetará si el delito que se atribuye o imputa al sospechoso tiene suficiente entidad a la vista de la injerencia en los derechos fundamentales que se va a producir con el archivo de los perfiles identificativos, que además se intercambiarán con otros Estados”, reputándose oscura la mención de “delito grave” y preferible la designación de tipos penales concretos, o un límite punitivo determinado y expreso. Por lo que respecta al control judicial del mantenimiento de los datos en el archivo, se estima “fundamental una comunicación puntual y fluida entre la autoridad judicial y el "responsable del fichero", de tal manera que en el momento en que concurra algún motivo de cancelación –v.gr.: absolución del imputado–, se proceda inmediatamente a la misma”, criticando la ausencia de un límite temporal máximo o absoluto claro. En materia de información de derechos al sospechoso, se echa de menos, en los protocolos policiales, la relativa al responsable del fichero –que no se concreta tampoco en la propia LO 10/2007, de qué manera o en qué supuestos podría ejercer los derechos de acceso, rectificación o cancelación, o qué posibilidades existen de "uso o cesión" de datos, incluyendo, precisamente, una referencia a la cesión a autoridades de otros Estados que es objeto de este tema.

- 2.2.1.3. **Datos dactiloscópicos**
- 2.2.1.4. **Datos de vehículos**
- 2.2.1.5. **Otros datos**
- 2.2.2. **Medidas de prevención de atentados terroristas**
 - 2.2.2.1. **Transmisión de información**
 - 2.2.2.2. **Escolta de seguridad en los vuelos**
- 2.2.3. **Medidas para la lucha contra la migración ilegal**
 - 2.2.3.1. **Envío de asesores en materia de documentación**
 - 2.2.3.2. **Apoyo en casos de repatriación**
- 2.2.4. **Otras formas de cooperación**
 - 2.2.4.1. **Patrullas comunes y otras formas de intervención conjunta**
 - 2.2.4.2. **Cruce de frontera**
 - 2.2.4.3. **Asistencia en caso de grandes eventos, catástrofes y accidentes graves**
 - 2.2.4.4. **Cooperación previa petición**
- 2.2.5. **Disposiciones sobre protección de datos de carácter personal**
 - 2.2.5.1. **Definiciones**
 - 2.2.5.2. **Nivel de protección de datos**
 - 2.2.5.3. **Principio de vinculación a fines y otros límites de utilización y tratamiento de datos**
 - 2.2.5.4. **Garantías de exactitud, actualidad y duración del almacenamiento de los datos**
 - 2.2.5.5. **Medidas técnicas y organizativas para garantizar la protección de los datos y su seguridad**

2.2.5.6. Documentación y registro

3. La parcial incorporación del Tratado de Prüm al marco jurídico de la Unión Europea

3.1. La Decisión JAI/615/2008

3.2. La Decisión JAI/616/2008

4. El principio de disponibilidad en el Programa de Estocolmo

5. Antecedentes penales

5.1. Introducción

5.2. Decisión Marco 2008/675/JAI

5.3. Decisión Marco 2009/315/JAI

5.4. Decisión 2009/316/JAI

En la Instrucción 3/2012 de la Secretaría General de la Administración de Justicia sobre determinadas cuestiones relativas a la organización y funcionamiento del Sistema de Registros Administrativos de Apoyo a la Administración de Justicia (SIRAJ), particularmente en relación con la integración de los Registros Centrales de Penados y Medidas Cautelares, Requisitorias y Sentencias no Firmes y de Protección de a las Víctimas de Violencia Doméstica, de 31 de julio de 2012, se hace referencia a la entrada en funcionamiento, el 27 de abril de 2012, del Sistema europeo de intercambio de antecedentes penales (ECRIS) como consecuencia de la plena entrada en vigor de la Decisión 2009/316/JAI del Consejo de 6 de abril de 2009 y la Decisión Marco 2009/315/JAI del Consejo de 26 de febrero de 2009, lo que “constituye un elemento fundamental para la aplicación de la Decisión Marco 2008/675/JAI del Consejo de 24 de julio de 2008, relativa a la consideración de las resoluciones condenatorias entre los Estados Miembros de la Unión Europea con motivo de un nuevo proceso penal.

El registro central de penados tiene ya en funcionamiento un sistema de petición de información de antecedentes penales de los ciudadanos de otros Estados de la Unión Europea, por lo que los juzgados y tribunales pueden solicitar estos antecedentes, cumplimentando la pantalla correspondiente de la aplicación: “consulta-nueva petición”. Cuando la nacionalidad corresponda a un país miembro de la UE se activará una alerta para petición de antecedentes a otro Estado. El registro central de penados cursará la petición y una vez recibida la contestación la remitirá electrónicamente al órgano judicial correspondiente. La entrada en funcionamiento de

ECRIS supone la incorporación de todos los Estados de la Unión Europea a este sistema de intercambio de información, mejorando la calidad y cantidad de los datos.

Para el correcto funcionamiento del sistema es fundamental la correcta identificación de las personas sobre las que se realiza la pregunta o sobre las que han sido sentenciadas en España. Es necesario hacer constar al menos: nombre y primer apellido, nacionalidad, localidad y fecha de nacimiento, y cuantos datos identificativos puedan existir, además lógicamente de los datos relativos a la condena y su ejecución. La ausencia de datos, su insuficiencia o el hecho de que puedan ser erróneos darán lugar a su no aceptación por el Estado de nacionalidad y por lo tanto a la imposibilidad de obtener el correspondiente certificado. Se ruega especial cuidado en este tema.

Cuando se trata de ciudadanos con nacionalidad distinta a la de alguno de los Estados miembros de la UE, el órgano judicial podrá solicitar también las anotaciones penales que puedan constar en otro Estado miembro de la UE, siempre que de la información existente en la causa se derive la posibilidad de que en dicho Estado pueda existir información relevante.

Anexo: Recursos de consulta sólo disponibles en castellano

Sin perjuicio de los recursos citados en el Nivel 3, los siguientes se encuentran disponibles en castellano y son, en su práctica totalidad, accesibles online.

- ACED FÉLEZ, E.: *Ejercicio y garantía del derecho a la protección de datos personales en el Convenio de Prüm*. Revista de Derecho Constitucional Europeo. Año 4, nº 7, enero-junio 2.007.
- BAR CENDÓN, A.: *El Tratado de Prüm y la inmigración ilegal*. Revista de Derecho Constitucional Europeo. Año 4, nº 7, enero-junio 2.007.
- CÁMARA VILLAR, G.: *La garantía de los derechos fundamentales afectados por la Convención de Prüm*. Revista de Derecho Constitucional Europeo. Año 4, nº 7, enero-junio 2.007.
- CASTILLEJO MANZANARES, R.: *Intercambio de información policial en el marco de la Unión Europea*, en La prueba en el espacio europeo de libertad, seguridad y justicia penal (libro electrónico). Aranzadi, 2008.

- DIETRICH PLAZA, C.: *El Tratado de Prüm en el marco de la regulación de protección de datos personales en la Unión Europea*. Revista de Derecho Constitucional Europeo. Año 4, nº 7, enero-junio 2.007.
- ETXEBERRÍA GURIDI, J.F.: *Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo*. Eguz Kilore nº 23, San Sebastián, diciembre 2009, págs. 357-366.
- FIGUEROA NAVARRO, C.: *Cooperación policial e intercambio de perfiles de ADN*. La Ley Penal nº 53, noviembre 2008.
- FREIXES SANJUÁN, T.: *Protección de datos y Globalización. La Convención de Prüm*. Revista de Derecho Constitucional Europeo. Año 4, nº 7, enero-junio 2.007.
- GÓMEZ SÁNCHEZ, Y.: *Los datos genéticos en el Tratado de Prüm*. Revista de Derecho Constitucional Europeo. Año 4, nº 7, enero-junio 2.007.
- HOYOS SANCHO, M.: *Archivo y conservación en registros policiales de muestras policiales de muestras biológicas y perfiles de ADN. Sentencia TEDH "S. y Marper contra el Reino Unido", de 4-12-2008 y la regulación española sobre obtención y registro de identificadores obtenidos a partir del ADN del sospechoso o imputado*. Estudios de Derecho Judicial. Consejo General del Poder Judicial, 2009.
- DEL MORAL TORRES, A.: *La cooperación policial en la Unión Europea: propuesta de un modelo europeo criminal*. Real Instituto Elcano.
- PALOMO DEL ARCO, A.: *Antecedentes penales (registro de condenas) en el ámbito europeo*, en *El proceso penal en la Unión Europea: garantías esenciales*, págs. 371-399. Ed. Lex Nova. Valladolid, 2008.
- PÉREZ FRANCESCH, J. L.: *Cooperación policial y judicial en la Convención de Prüm*. Revista de Derecho Constitucional Europeo. Año 4, nº 7, enero-junio 2.007.
- PRIETO RAMÍREZ, L. M.: *La Ley Orgánica reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN*. Revista Jurídica Aranzadi. Nº 747, 13 de marzo de 2.008.
- REMOTTI CARBONELL, J. C.: *Las medidas contra el terrorismo en el marco del Tratado de Prüm*. Revista de Derecho Constitucional Europeo. Año 4, nº 7, enero-junio 2.007.

- **RODRÍGUEZ, J.M y SORROZA BLANCO, A.:** *El espacio de libertad, seguridad y justicia y la próxima Presidencia española de 2010. Parte 1ª. La implementación del Tratado de Lisboa y el Programa de Estocolmo.* ARI nº 173/2009, de 22/12/2009. Real Instituto Elcano.
- **SORROZA, A.:** *La seguridad interior en la UE: diez años después del 11-S.* ARI 127/2011, 07/09/2011. Real Instituto Elcano
- **VUELTA SIMON, S.:** *El Tratado de Prüm, nueva herramienta de cooperación policial en Europa.* Curso Virtual de Cooperación Judicial Penal en Europa, Edición 2.009.
- **ZAMBRANO GÓMEZ, E.:** *La regulación de los ficheros policiales en España y su tratamiento en la Convención de Prüm. La perspectiva de las autoridades nacionales de protección de datos.* Revista de Derecho Constitucional Europeo. Año 4, nº 7, enero-junio 2.007.
- **ZILLER, Jacques.** *El Tratado de Prüm.* Revista de Derecho Constitucional Europeo. Año 4, nº 7, enero-junio 2.007 (versión española del original francés).

Fernando Martínez Pérez
 María Poza Cisneros
 1 de septiembre de 2012