

EL TRATADO DE PRÜM EN EL MARCO DE LA REGULACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES EN LA UNIÓN EUROPEA*

Cristina Dietrich Plaza**

SUMARIO

- 1.- *Introducción.*
- 2.- *El marco de la protección de datos personales en la Unión Europea. La distinción entre materias referidas al primer y tercer pilar comunitario.*
- 3.- *El principio de disponibilidad en el Programa de La Haya.*
- 4.- *Referencia a los sistemas de información en la Unión Europea. El Sistema de Información de Schengen.*
- 5.- *Las propuestas de Decisión Marco del Consejo relativas al principio de disponibilidad y a la protección de datos en el tercer pilar comunitario.*
- 6.- *La remisión al derecho interno en el Tratado de Prüm.*
- 7.- *Conclusiones.*

1. INTRODUCCIÓN

El 27 de mayo de 2005 se firmó en la ciudad alemana de Prüm un Tratado internacional entre siete Estados miembros de la Unión Europea (el Reino de Bélgica, la República Federal de Alemania, el Reino de España,

* Este artículo es resumen de la ponencia realizada por la autora en la Jornada sobre Derechos Fundamentales y Convención de Prüm. Protección de Datos y Globalización, realizado en Barcelona, el 15 de diciembre de 2006.

** Auditora de la Asesoría Jurídica de la Agencia Catalana de Protección de Datos. Profesora asociada del Área de Derecho Constitucional de la Universidad Autónoma de Barcelona.

la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos y la República de Austria), relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal (en adelante, el Tratado)¹. Más recientemente, en fecha 5 de diciembre de 2006, han iniciado el proceso para adherirse al Tratado diversos países de la Unión Europea, entre otros, Italia, Portugal y Finlandia. En la reunión celebrada en Bruselas en esta fecha, se firma también el Acuerdo Técnico de Ejecución de Tratado de Prüm, previsto en el artículo 44 del mismo.

Por lo que respecta a España, 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.

Mediante este Tratado los Estados firmantes pretenden reforzar su cooperación, incrementando el intercambio de información a través de determinados puntos de contacto nacionales en ámbitos de naturaleza ciertamente diversa, como son la lucha contra el terrorismo, la delincuencia organizada y la migración ilegal.

Si bien el artículo 1.1 del Tratado dispone que las Partes pretenden “reforzar la cooperación transfronteriza”, no se ha optado por utilizar un mecanismo propio del Derecho comunitario, como es el de la cooperación reforzada previsto en el Tratado de la Unión Europea, sino un mecanismo ajeno al mismo, como es un tratado internacional².

¹ Ver el texto del Tratado y la Declaración que España va a formular en el momento de su ratificación, en el *Boletín Oficial de las Cortes Generales*, serie A, núm. 230, de 17 de febrero de 2006. Por lo que respecta al Dictamen emitido por la Comisión de Asuntos Exteriores del Congreso de los Diputados, por el que se propone la pertinente concesión de autorización solicitada por el Gobierno al amparo de lo que dispone el artículo 94.1 de la Constitución para que el Estado pueda obligarse internacionalmente, ver el *Boletín Oficial de las Cortes Generales*, serie C, núm. 156-2, de 11 de abril de 2006.

² Los artículos 43 a 45 del Tratado de la Unión Europea (TUE) prevén las disposiciones relativas a la “cooperación reforzada”, concepto que fue introducido en el TUE por el Tratado de Amsterdam. Es posible recurrir a la cooperación reforzada como mínimo entre ocho Estados miembros de la Unión, en los ámbitos de aplicación del Tratado constitutivo de la Comunidad Europea, así como en la cooperación policial y judicial en materia penal, por tanto, en materias del primer y tercer pilar comunitarios. En cuanto a la Política Exterior y de Seguridad Común (PESC), correspondiente al segundo pilar de la UE, no se prevé este mecanismo, sino la adopción por unanimidad de las decisiones, pudiendo los Estados utilizar la “abstención constructiva”, según dispone el artículo 23 TUE. En función de que la cooperación reforzada se refiera a materias del primer o tercer pilar, se exigen determinadas condiciones, como se precisa en los artículos citados, así como en los artículos 40 y siguientes, por lo que respecta al tercer pilar.

Independientemente de que se haya optado por recurrir a la firma de un tratado internacional en vez de utilizar otros mecanismos propios del derecho comunitario, el hecho es que las disposiciones del Tratado de Prüm tienen una profunda repercusión en la materia que nos ocupa, esto es, la protección de datos de carácter personal, puesto que el Tratado se basa en el intercambio de información entre los Estados, incluyendo en buena parte datos de carácter personal.

Por tanto, es necesario establecer el encaje del Tratado en el entramado normativo aplicable a la protección de datos en el marco de la Unión Europea. Para ello habrá que hacer referencia a los pilares comunitarios, puesto que en función de que una materia determinada pertenezca a uno u otro pilar comunitario, las normas de protección de datos de referencia, como se verá, van a ser diferentes.

Por otra parte, el Tratado de Prüm se ha considerado como una nueva manifestación del principio jurídico de disponibilidad, que surge a nivel comunitario en el Programa de La Haya, adoptado por el Consejo Europeo de noviembre de 2004, relativo a la Consolidación de la Libertad, la Seguridad y la Justicia en la Unión Europea, y desarrollado posteriormente a través de un Plan de acción del Consejo y de la Comisión³.

El principio de disponibilidad, según el cual la información necesaria en el marco de la cooperación policial y judicial, en concreto, para la lucha contra la delincuencia, puede atravesar las fronteras interiores de los países de la Unión sin encontrar obstáculos, se ha desarrollado en varias propuestas normativas de la Unión Europea, que serán comentadas en este artículo, y encuentra un nuevo desarrollo en el Tratado de Prüm. Si bien en el Tratado la referencia al principio de disponibilidad no se encuentra de forma explícita, los Estados parte exponen en uno de sus considerandos la asunción de un papel pionero en la consecución del máximo nivel posible de cooperación, en aras del desarrollo de la cooperación europea y sin perjuicio del Tratado de la Unión Europea y del Tratado constitutivo de la Unión Europea, “en particular, mediante un mejor intercambio de información, especialmente en el ámbito de la lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal”. Ello supone sin duda un nuevo desarrollo del mencionado principio de disponibilidad, de forma paralela a otras normas enmarcadas en el derecho de la Unión.

³ Publicado en el *DOUE* serie C 53, de 3.3.2005. Complementariamente, consultar: Plan de Acción del Consejo y la Comisión por el que se aplica el Programa de La Haya sobre refuerzo de la libertad, la seguridad y la justicia en la Unión Europea, *DOUE* C 198, de 12.8.2005.

Es necesario, además, distinguir el contenido del Tratado de Prüm de otros sistemas de intercambio de información que ya existen en el marco de la Unión Europea. En los últimos años, se han desarrollado diversos sistemas de información que atañen a materias que también van a ser objeto de intercambio de información en el Tratado de Prüm, como son la migración ilegal o la delincuencia transfronteriza. Estos sistemas de intercambio de información a gran escala pueden contener sus propias normas de protección de datos, que deberán interpretarse en coordinación con el marco jurídico aplicable en esta materia, e incluso prevén mecanismos de protección de datos específicos, como por ejemplo las Autoridades Comunes de Control de Schengen, Eurojust o Europol, en las que participan diversas autoridades de protección de datos de los países que forman parte de estos sistemas de información y que tienen como objetivo garantizar una adecuada protección de datos en el tratamiento que de éstos se realicen en dichos sistemas⁴.

Actualmente, además, se están desarrollando paralelamente dos propuestas de Decisión Marco que afectan al tercer pilar comunitario, y que van a tener una repercusión clave en materia de protección de datos. Se trata de la Propuesta de Decisión marco del Consejo sobre intercambio de información en virtud del principio de disponibilidad (COM (2005) 490 final) y de la Propuesta 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 (COM (2005) 475 final). En el momento en que estas propuestas pasen a concretarse en normas vigentes del derecho de la Unión Europea, formarán parte del marco jurídico al que tendrán que ajustarse las previsiones del Tratado de Prüm.

Efectivamente el Tratado parte de la base, como se prevé en su artículo 47, que las disposiciones que contiene sólo serán aplicables en la medida en que sean compatibles con el derecho de la Unión Europea, y por tanto, en relación con la protección de datos, deberán tenerse en cuenta las diversas normas jurídicas que han sido desarrolladas a nivel comunitario y afectan a dicha materia, así como las normas citadas que se están desarrollando y que, en el momento de su entrada en vigor, van a formar parte del marco jurídico aplicable a las disposiciones del Tratado que afectan a la protección de datos de carácter personal⁵.

⁴ Por lo que respecta a estas Autoridades de Control, nos remitimos, entre otras fuentes de información, a: <http://europoljsb.consilium.europa.es/default.asp?lang=es> - <http://www.schenga-ja-dataprotection.org/> - <http://eurojust.europa.eu/>

⁵ Artículo 47.1 del Tratado de Prüm: *“Las disposiciones del presente Tratado sólo serán aplicables en la medida en que sean compatibles con el derecho de la unión Europea. Si en*

En conclusión, los Estados parte del Tratado han optado por recurrir a un instrumento ajeno al marco institucional de la Unión Europea, lo cual ha sido objeto de críticas por parte, entre otros, del Supervisor Europeo de Protección de Datos (en adelante, SEPD)⁶. El SEPD, en su Dictamen a la propuesta de Decisión marco del Consejo sobre intercambio de información en virtud del principio de disponibilidad, refiriéndose al Tratado de Prüm, ha expuesto su disconformidad con el proceso que ha conducido a la aprobación de dicho Tratado, fuera del marco institucional de la Unión Europea puesto que ello supone, entre otras cosas, la falta de participación del Parlamento Europeo en dicho proceso, si bien es cierto que, en referencia a España, la Agencia Española de Protección de Datos presentó un informe preceptivo al Parlamento español relativo al Tratado de Prüm⁷. Por tanto, los parlamentos estatales sí han tenido la posibilidad de valorar dicho Tratado.

El Tratado somete la aplicación de sus disposiciones a su compatibilidad con el derecho de la Unión Europea, y además tiene la voluntad de incorporar el régimen que establece al marco jurídico de la Unión Europea⁸,

el futuro la UE adoptara normas que puedan afectar al ámbito de aplicación del presente Tratado, las disposiciones correspondientes del presente Tratado dejarán de aplicarse en beneficio del derecho de la UE. Las Partes Contratantes podrán modificar o reemplazar las disposiciones del presente Tratado a la luz de las nuevas disposiciones pertinentes del derecho de la Unión Europea.”

⁶ El Supervisor Europeo emite su dictamen en base a lo que dispone 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, y lo que dispone el Reglamento (CE) nº 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 (DOCE serie L 8, de 12.1.2001).

⁷ El Dictamen se publicó en el DOUE serie C 116, de 17.5.2006. En concreto: *“El SEPD 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). Ello incluye la perspectiva de la protección de datos (...). Las instituciones de la Unión Europea no tienen la oportunidad de valorar - antes de que se establezca el sistema- el impacto de las elecciones políticas en la protección de datos personales”.*

⁸ Según consta en el Preámbulo del Tratado, en su artículo 1.4: *“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”.*

por tanto es innegable que, una vez escogido un camino diferente al del marco institucional comunitario, hay que tener presente el actual marco y entramado de normas jurídicas de distinta índole que, en la Unión Europea, están afectando a la transmisión de información entre los Estados de la Unión y, más en concreto, están afectando al derecho fundamental a la protección de datos de carácter personal.

Finalmente, también veremos que el Tratado hace una remisión constante al derecho interno de las partes (entre otros, el artículo 34 del mismo). Por lo que respecta a la protección de datos personales, habrá que tener en cuenta las previsiones que las normas internas respectivas establezcan en dicha materia.

2. EL MARCO DE LA PROTECCIÓN DE DATOS PERSONALES EN LA UNIÓN EUROPEA⁹. LA DISTINCIÓN ENTRE MATERIAS REFERIDAS AL PRIMER Y TERCER PILAR COMUNITARIO

En primer lugar debe hacerse referencia al Convenio 108 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, así como a su Protocolo adicional, de 8 de noviembre de 2001, que todavía no ha sido firmado ni ratificado por España, aunque podría considerarse que su contenido forma parte del desarrollo legislativo de la protección de datos que se ha producido en España.

El Tratado hace mención expresa de este Convenio en su artículo 34, según el cual en relación con el tratamiento de datos de carácter personal transmitidos o que se transmitan en virtud del mismo, cada Parte Contratante garantizará que su derecho interno ofrezca un nivel de protección de datos equivalente como mínimo al que resulta de este Convenio. Así pues, el Convenio de 1981 se configura como estándar mínimo de protección en el tratamiento de datos derivado de la aplicación del Tratado de Prüm.

⁹ Derecho fundamental presente en la Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01), *DOCE* serie C de 18.12.2000. En concreto, en su artículo 8, dispone que:

“1. Toda persona tiene derecho a la protección de datos de carácter personal que la conciernan.

2. Estos datos se tratarán 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. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. *El respeto de estas normas quedará sujeto al control de una autoridad independiente”.*

En el marco de la Unión Europea se han desarrollado varias directivas que afectan a la protección de datos personales, de las que destacamos la Directiva 95/46/CE del Parlamento europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas por lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

Finalmente debe tenerse en cuenta el desarrollo legislativo que a nivel interno realicen los países de la Unión, en el caso de España, principalmente a través de la Ley Orgánica 15/1999, de protección de datos de carácter personal¹⁰.

Para determinar el marco aplicable a la protección de datos en la Unión Europea, es necesario hacer una distinción entre el primer y tercer pilar comunitario, puesto que en función de que un tratamiento de datos personales se realice en relación con materias de uno u otro pilar, las normas aplicables en cuanto a la protección de datos serán diferentes.

El concepto de “pilares” se utiliza en el Tratado de la Unión Europea para definir la arquitectura de la Unión. En concreto el primer pilar comunitario corresponde a las tres comunidades (CEE, EURATOM y CECA), el segundo pilar corresponde a la política exterior y de seguridad común (PESC), regulada en el Título V del Tratado de la Unión Europea, y finalmente el tercer pilar, a la cooperación policial y judicial en materia penal (regulada en el Título VI de TUE).

Básicamente, las materias relativas a visados, asilo, inmigración y otras políticas relacionadas con la libre circulación de las personas, pertenecen al primer pilar, mientras que las de prevención y lucha contra el terrorismo, el tráfico de personas, la cooperación policial y aduanera, la regulación de Europol, así como la cooperación judicial en materia penal, pertenecen al tercer pilar.

Los tres pilares comunitarios funcionan conforme a procedimientos decisorios diferentes. Procedimiento comunitario para el primer pilar, (en el que la Comisión es la única que puede presentar propuestas al Consejo y

¹⁰ En relación con la Comunidad Autónoma de Cataluña, cabe citar los artículos 31 y 156 del actual Estatuto de Autonomía, en conexión con la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos.

al Parlamento, y la mayoría cualificada basta para la adopción de los actos del Consejo; papel activo del Parlamento Europeo; uniformidad de interpretación del derecho comunitario garantizada por el Tribunal de Justicia), y procedimiento intergubernamental para los otros dos pilares (en los que la Comisión y los Estados miembros comparten el derecho de iniciativa, y la unanimidad en el Consejo es en principio necesaria; por lo que respecta a dichos pilares se prevé un papel consultivo del Parlamento Europeo y una intervención limitada del Tribunal de Justicia).

En relación con la protección de datos de carácter personal, debe tenerse en cuenta que según prevé el artículo 3.2 de la Directiva 95/46/CE, sus disposiciones no se aplican al tratamiento de datos personales que se efectúen en el ejercicio de actividades no incluidas en el ámbito de aplicación del Derecho comunitario, como las que se prevén en las disposiciones de los Títulos V y VI del TUE y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (...) y las actividades del Estado en materia penal. Por tanto, la Directiva de 1995 no se aplica a materias propias del tercer pilar comunitario.

Como veremos más adelante, se está desarrollando una propuesta de Decisión Marco que vendría a ser el marco jurídico de referencia en materia de protección de datos en el tercer pilar, equivalente a la citada Directiva por lo que respecta al desarrollo de materias propias del primer pilar¹¹.

En definitiva, teniendo en cuenta las materias desarrolladas por el Tratado de Prüm, las directivas citadas, actualmente en vigor, no resultarían de aplicación, y por tanto, mientras no se desarrollen las nuevas decisiones marco, el Tratado ha establecido una remisión al Convenio 108 del Consejo de Europa, como primera norma de referencia, en el citado artículo 34. En este sentido, por tanto, el Tratado remite a la protección mínima que el derecho interno, al que haremos referencia más adelante, deberá establecer en materia de protección de datos.

¹¹ Se ha apuntado en ocasiones la dificultad, por lo que respecta a la protección de datos, de concretar la finalidad en cada caso de un tratamiento determinado de datos, para definir claramente si nos encontramos en una materia propia del primer o tercer pilar comunitario, ya que ello es clave para determinar las normas comunitarias de referencia que van a ser aplicables. En este sentido destaca la petición por parte de las Autoridades de Protección de Datos Europeas, de armonizar y equiparar la protección de datos en ambos pilares. (Ver al respecto la Declaración en: *Spring Conference of European Data Protection Authorities*, Krakow, 25-26 abril 2005).

3. EL PRINCIPIO DE DISPONIBILIDAD EN EL PROGRAMA DE LA HAYA

El principio de disponibilidad se desarrolla en el Programa de La Haya de noviembre de 2004 y tiene como orientaciones específicas la consolidación de la libertad (en relación, entre otros ámbitos, con la ciudadanía de la Unión, la política de asilo, migración y fronteras, el sistema europeo común de asilo, la migración legal y la lucha contra el empleo ilegal, la gestión de los flujos migratorios, los controles en frontera y la lucha contra la inmigración ilegal), la consolidación de la seguridad (consagrando la mejora del intercambio de información, la lucha contra el terrorismo, la cooperación policial y la gestión de crisis internas de la Unión Europea con repercusiones transfronterizas o la prevención de la delincuencia) así como la finalidad de reforzar la justicia a través de la cooperación judicial en materia penal, entre otras medidas.

El principio de disponibilidad establece básicamente que la información de que disponen los países miembros debe intercambiarse con la mayor celeridad posible entre los servicios policiales de la UE, salvando las previsiones que sean necesarias sobre protección de datos personales, y para conseguir este intercambio de información, se prevé el uso de nuevas tecnologías que lógicamente va aparejado a la consecución de dicha finalidad¹².

El principio de disponibilidad recogido en dicho programa, así como en diversas propuestas que se han presentado posteriormente, consiste por tanto en el incremento progresivo del intercambio de información entre los Estados de la Unión para el cumplimiento de diversas tareas legales relacionadas con las materias que se han apuntado, las cuales también forman el núcleo de los objetivos que pretende conseguir el Tratado de Prüm. Como se precisa en el punto 2.1 del citado Programa de La Haya:

«Con efectos a partir del 1 de enero de 2008, el intercambio de dicha información deberá regirse (...) respecto del principio de disponibilidad, lo que significa que, en todo el territorio de la Unión, un funcionario de policía de un Estado miembro que necesite información para llevar a cabo sus

¹² El Consejo de Justicia y Asuntos de Interior (JAI) inicia diversos trabajos de desarrollo del principio de disponibilidad en los siguientes ámbitos: ADN, impresiones dactilares, balística, registros de vehículos y números de teléfono, datos mínimos de personas contenidos en registros civiles. El Comité del Artículo 36 de TUE (también denominado CATS), como grupo de trabajo del Consejo, que tiene 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).

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».

Nos encontramos pues ante la consagración y progresiva incorporación a diversos textos jurídicos y políticas de la Unión Europea de un principio de disponibilidad de la información de que disponen los Estados, el cual va a tener una repercusión incuestionable en materia de protección de los datos personales de los ciudadanos afectados de un modo u otro por dichas políticas propias del derecho comunitario o desarrolladas por mecanismos jurídicos ajenos formalmente al derecho comunitario, como es el Tratado de Prüm.

Este principio de disponibilidad está presente, entre otros textos, en la Propuesta 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, así como en la Propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad, como tendremos ocasión de comentar¹³.

El hecho de que los tres campos de actuación del Tratado de Prüm, esto es, la lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, sean objeto paralelamente de actuaciones de la Unión Europea, en ambos casos con la progresiva implantación del citado principio, plantea ciertas dudas respecto a las previsiones relativas a la protección de datos, en el sentido de si van a ser suficientes las previsiones que el actual marco jurídico prevé, o si van a tener que reforzarse de algún modo.

No debe olvidarse que en la Unión Europea existe actualmente la tendencia a crear, o como mínimo a reflexionar sobre la posibilidad de crear nuevas interconexiones entre grandes sistemas de información que ya existen en la actualidad, y a los que nos referiremos más adelante, principalmente el Sistema de Información de Schengen, que está siendo revisado en la actualidad para desarrollar el llamado "SIS II" (Sistema de Información Schengen de segunda generación), así como el Sistema de información de

¹³ Las referencias de las dos Propuestas de decisión marco, respectivamente, son: COM (2005) 475, y COM (2005) 490.

visados (VIS)¹⁴ o el Sistema Eurodac, relativo a la comparación de impresiones digitales de solicitantes de asilo¹⁵.

Si bien es cierto que en el Tratado de Prüm no se explicitan determinadas interacciones o accesos directos a dichos sistemas de información, es innegable que éstos comparten en buena medida objetivos comunes con el Tratado, y por tanto es pertinente tener en cuenta las previsiones de dichos sistemas de información en relación con la protección de datos personales y su repercusión en las previsiones de intercambio de información que se van a realizar entre los Estados parte del Tratado de Prüm. En este sentido, la posibilidad de que en el futuro pudieran preverse algunas interacciones entre las informaciones y datos personales tratados en el marco de estos sistemas de información y las bases de datos creadas a partir del Tratado, deberá ser objeto de una profunda reflexión.

Por lo que respecta al Tratado de Prüm, se hace referencia continua a la mejora del intercambio de información entre los Estados miembros, a través del acceso y consulta automatizada de determinadas bases de datos, y en este sentido, el principio de disponibilidad está presente en el Tratado. Así lo expone el 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 disponibilidad¹⁶.

¹⁴ Respecto al Sistema de Información de Visados (VIS), consultar: Decisión 2004/512/CE del Consejo, de 8 de junio de 2004, por la que se establece este sistema. *Diario Oficial* L 213 de 15.6.2004. Consultar también la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al sistema de información sobre los visados (VIS) y el intercambio de datos entre los Estados miembros sobre los visados de corta duración (COM (2005) 835 final). Respecto a esta Propuesta de Reglamento, se citan el Dictamen 2/2005, del Grupo del Artículo 29 sobre Protección de Datos (ref.- 1022/05/ES. WP 110), así como el Dictamen del SEPD, en *DOUE* serie C 181, de 23.7.2005.

¹⁵“Eurodac” por su parte, es un sistema de comparación de impresiones dactilares de los solicitantes de asilo e inmigrantes clandestinos con el fin de facilitar la aplicación del Convenio de Dublín. Respecto a Eurodac, ver el Reglamento CE nº 2725/2000 del Consejo, de 11.12.2000, publicado en el *DOCE* serie L 316, de 15.12.2000. El Convenio de Dublín se puede consultar en el *DOCE* serie C 254, de 19.8.1997. Este Convenio queda afectado por el Reglamento (CE) nº 343/2003 del Consejo, de 18 de febrero de 2003, que establece los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados miembros por un nacional de un tercer país. *Diario Oficial* L 50 de 25.12.2003.

¹⁶ Como destaca el SEPD en el citado Dictamen: *“En sí mismo, el principio de disponibilidad es sencillo. La información de que disponen determinadas autoridades en un Estado miembro debe facilitarse también a las autoridades equivalentes de otros estados miembros. La información debe intercambiarse con la mayor rapidez y facilidad posibles entre las autoridades de los Estados miembros y preferiblemente, permitiendo el acceso directo en línea”*.

La base jurídica del principio de disponibilidad se encuentra en el Título VI del Tratado de la Unión Europea, sobre Disposiciones relativas a la cooperación policial y judicial en materia penal, (relativo al tercer pilar comunitario) en concreto, en el artículo 30.1.b), que dispone lo siguiente:

«La acción en común en el ámbito de la cooperación policial incluirá:
(...)

b) La recogida, almacenamiento, tratamiento, análisis e intercambio de información pertinente, en particular mediante Europol, incluida la correspondiente a informes sobre operaciones financieras sospechosas que obre en poder de servicios con funciones coercitivas, con sujeción a las disposiciones correspondientes en materia de protección de datos personales;»

Así como en el artículo 34.2.b), que dispone:

«El Consejo dispondrá y fomentará, en la forma y según los procedimientos oportunos tal como se establece en el presente título, la cooperación pertinente para la consecución de los objetivos de la Unión. A tal fin, a iniciativa de cualquier Estado miembro o de la Comisión, el Consejo podrá, por unanimidad:

(...)

b) adoptar decisiones marco para la aproximación de las disposiciones legales y reglamentarias de los Estados miembros. Las decisiones marco¹⁷ obligarán a los Estados miembros en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios. No tendrán efecto directo;»

El Consejo Europeo concede un carácter prioritario a la aplicación del principio de disponibilidad a partir de las previsiones concretadas en el Programa de La Haya, aunque 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. El principio de disponibilidad se considera norma común a la hora de intercambiar y compartir información entre los servicios policiales de los Estados de la Unión. Con el fin de que la estructura de intercambio de información propuesta en dicho Programa pueda estar lista el 1 de enero de 2008, se pide a la Comisión que presente antes de 2005 propuestas adecuadas.

¹⁷ Respecto a las Decisiones marco, tener en cuenta el artículo 39.1 TUE, según el cual el Consejo consultará al Parlamento Europeo antes de adoptar cualquier medida mencionada en las letras b), c) y d) del apartado 2 del artículo 34. El Parlamento Europeo emitirá su dictamen dentro de un plazo que podrá fijar el Consejo y que no será inferior a tres meses. En ausencia de dictamen dentro de ese plazo, se prevé que el Consejo podrá actuar.

Como se ha avanzado, el Tratado de Prüm se ha planteado, si bien de forma ajena a las iniciativas impulsadas desde la Unión, como una nueva manifestación de este principio de disponibilidad. Los tres objetivos del Tratado de Prüm, esto es, la lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, son objetivos también presentes en el Programa de La Haya, del que se destacan a continuación algunas apreciaciones.

Respecto a la lucha contra el terrorismo¹⁸, el Programa de La Haya considera que es preciso que los Estados miembros de la Unión no limiten sus actividades a mantener la seguridad propia, sino que se planteen también la seguridad de la Unión en su conjunto. Entre otros objetivos, ello supone que los Estados deben atraer inmediatamente la atención de las autoridades competentes de los otros Estados miembros sobre cualquier información de que dispongan sus servicios, en relación con amenazas para la seguridad interior de dichos Estados. De ello parece derivarse una voluntad de que los Estados se avancen a la petición concreta de información puntual por parte de otros Estados miembros, y actúen por propia iniciativa a la hora de poner en conocimiento de otros Estados determinada información relevante.

La posibilidad de “avanzarse” a peticiones concretas está presente también en el Tratado de Prüm, en concreto en su artículo 16 según el cual, con en objeto de prevenir atentados terroristas las Partes Contratantes podrán transmitir a los otros Estados, con arreglo al derecho interno, en casos concretos, sin necesidad de petición previa, los datos de carácter personal y la descripción de los hechos que justifican dicha transmisión, cuando exista la presunción de que las personas de que se trate van a cometer delitos relacionados con actos de terrorismo¹⁹.

El Programa de La Haya prevé en este sentido que se mantendrá el alto nivel de intercambio de información entre los servicios de seguridad, aunque éste deberá mejorarse teniendo en cuenta el principio general de disponibilidad al que se viene haciendo referencia.

Respecto a la delincuencia transfronteriza, presente como objetivo en el Tratado, también ha sido objeto de especial atención en el Programa de La Haya. Se pretende mejorar la transmisión de información entre los Estados para luchar contra la delincuencia organizada transfronteriza. Según

¹⁸ En esta materia, se cita la Decisión marco 2002/475/JAI del Consejo, de 13 de junio de 2002, relativa a la lucha contra el terrorismo (*DOUE* serie C, 164, de 22.6.2002).

¹⁹ El Tratado se remite a la Decisión Marco núm. 2002/475/JI del Consejo de la Unión Europea, de 13 de junio de 2002, para la lucha contra el terrorismo (artículos 1 a 3).

el Programa, la lucha efectiva contra la delincuencia organizada transfronteriza y otras formas graves de delincuencia requiere una cooperación práctica intensificada entre las autoridades policiales y aduaneras de los Estados miembros y con Europol, y en este sentido el Consejo Europeo insta a los Estados a que capaciten a Europol para que, en cooperación con Eurojust, desempeñe un papel clave en la lucha contra las formas graves de delincuencia transfronteriza (organizada o no organizada). Se insta en este sentido a que los Estados mejoren la calidad de sus datos policiales con la ayuda de Europol.

Parece claro en este sentido que en cuanto a la cooperación policial en materia de lucha contra la delincuencia organizada el Programa de La Haya apunta al desarrollo del principio de disponibilidad, posiblemente, a través de nuevas interrelaciones entre diferentes sistemas de información²⁰.

Finalmente, por lo que respecta a la migración ilegal, otro de los objetivos comunes del Tratado de Prüm y del Programa de La Haya, este último explicita la necesidad de reforzar la gestión de flujos migratorios, incluida la lucha contra la inmigración ilegal, con medidas de seguridad que establezcan un nexo eficaz entre los trámites de solicitud de visados y los de entrada y salida en pasos fronterizos exteriores. Para lograrlo, se apunta a la necesidad de buscar soluciones armonizadas a nivel de la UE en materia de identificadores y datos biométricos. En este sentido se buscaría un máximo de eficacia e interoperabilidad de los sistemas de información de la UE para hacer frente a la inmigración ilegal.

Así pues, se constata una vez más que la actuación que la UE pretende desarrollar en diversas materias de manera armonizada a nivel comunitario, se ve desarrollada de forma paralela por el Tratado de Prüm.

Conviene señalar que, respecto del desarrollo global del principio de disponibilidad, el programa de La Haya dispone que deberán cumplirse estrictamente una serie de condiciones que cualifica de imprescindibles²¹. Nuevamente podría plantearse la posibilidad de que estos requisitos de protección de la información y de los datos personales, tengan una diferente aplicación en las normas que vayan surgiendo a nivel comunitario, y en el desarrollo del Tratado de Prüm, que, insistimos en ello, no surge de la

²⁰ En este sentido, el Plan de Acción del Consejo y la Comisión por el que se aplica el Programa de La Haya, cita como objetivos, entre otros, el intercambio de información entre autoridades policiales y judiciales guardando un equilibrio adecuado entre derecho a la intimidad y seguridad, así como el desarrollo de la instauración del principio de disponibilidad de la información pertinente a efectos policiales, y el desarrollo de vínculos entre SIS II y el Sistema de información de Europol.

propia UE, sino de una cooperación específica entre determinados Estados miembros de la Unión.

A ello se añade una última consideración del Programa de La Haya. Al referirse a los métodos de intercambio de información, se considera que éstos deberán hacer pleno uso de las nuevas tecnologías y adaptarse a cada tipo de información, si procede a través del acceso recíproco a las bases de datos o del acceso directo (en línea) incluso para Europol, a las bases de datos centrales existentes, tales como el Sistema de Información de Schengen. Sólo deberán crearse nuevas bases de datos europeas centralizadas sobre la base de estudios que hayan demostrado su valor añadido. Podríamos preguntarnos, en este sentido, si la creación de nuevas bases de datos de ADN prevista en el Tratado de Prüm, si bien no se trata de una nueva gran base de datos, sino de bases de datos estatales, podría superar la exigencia de “valor añadido” exigido por el Programa de La Haya.

4. REFERENCIA A LOS SISTEMAS DE INFORMACIÓN EN LA UNIÓN EUROPEA. EL SISTEMA DE INFORMACIÓN DE SCHENGEN

Existen varios instrumentos jurídicos en la Unión Europea que vienen siendo desarrollados desde hace años, y que en cuanto al intercambio de información y datos personales que implica su desarrollo, son en buena medida una manifestación del principio de disponibilidad²¹.

En el Programa de La Haya se apuesta por la interoperabilidad entre el sistema de información de Schengen (SIS II), el sistema de información de visados (VIS) y el sistema EURODAC. Respecto a las posibilidades que se

²¹ En concreto: El intercambio de información sólo tendrá lugar para el cumplimiento de tareas legales. Debe garantizarse la integridad de los datos que deban intercambiarse. Necesidad de proteger las fuentes de información y de garantizar la confidencialidad de los datos en todas las etapas del intercambio, y la aplicación de normas comunes para el acceso a los datos y normas técnicas comunes. Supervisión del respecto de la protección de datos y garantía de un adecuado control previo y posterior al intercambio de información. Garantía de protección contra el uso indebido de los datos personales y el derecho a la corrección de los datos personales incorrectos.

²² Así lo apunta el SEPD, en su referido Dictamen sobre la propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad, en la consideración preliminar 11: *“La disponibilidad de información policial y judicial a través de las fronteras interiores de la UE se facilitará asimismo mediante otros instrumentos jurídicos como las propuestas relativas a la segunda generación del Sistema de Información de Schengen (SIS II), la propuesta sobre el acceso a la consulta del Sistema de Información de Visados (VIS) y la propuesta de Decisión marco relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros. (...)”*

plantean de establecer interconexiones entre grandes sistemas de información, cabe citar la Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 24 de noviembre de 2005, sobre una mayor eficacia, interoperabilidad y sinergia entre las bases de datos europeas en el ámbito de la Justicia y los Asuntos de Interior (JAI) (COM(2005) 567) presentada por la Comisión el 25 de enero de 2005²³.

La Comunicación citada se refiere a los tres principales sistemas de información de que dispone en la actualidad la Unión Europea, esto es, el Sistema de Información Schengen (SIS II), el Sistema de Información de Visados (VIS)²⁴ y EURODAC²⁵.

Plantea diversas posibilidades que podrían tratarse para una más eficaz utilización de dichos sistemas, e incluso la creación de otros nuevos. Así, plantea las posibilidades de incrementar la interoperabilidad técnica (capacidad para compartir e intercambiar información y conocimientos de los sistemas de información), la conectividad (conexión de dispositivos para transferir datos) y la sinergia (que se define como una mejora de la interrelación en sus dimensiones técnicas, económicas y organizativas), todo ello remitiendo al principio de disponibilidad que ya conocemos, esto es, que las autoridades responsables de la seguridad de un Estado miembro o incluso Europol, pudieran obtener de otro Estado miembro la información que necesitan, si es posible acceder a ella²⁶.

En esta Comunicación, se explicita que cada uno de estos tres sistemas de información persiguen finalidades concretas, y por tanto utilizan datos personales que no tienen por qué ser los mismos, puesto que se tratarán en función de la finalidad de cada sistema.

²³ COM (2005) 597. Comunicación transmitida al Consejo y al Parlamento Europeo en fecha 24.11.2005.

²⁴ La base jurídica del VIS se encuentra en la Decisión 2004/512/CE del Consejo, de 8 de junio de 2004, que establece este sistema de información (*DOUE* L 213, de 15.6.2004), y por lo que respecta a una segunda etapa del mismo, en la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al VIS y el intercambio de datos entre los Estados miembros sobre los visados de estancia corta (COM (2005) 835. Al respecto, ver el Dictamen del Supervisor Europeo de Protección de Datos, publicado en *DOUE* C 181 de 23.7.2005, así como el Dictamen 2/2005 del grupo del Artículo 29 sobre protección de datos, de 23 de junio de 2005.

²⁵ EURODAC tiene como objetivo ayudar a determinar el Estado miembro responsable de las solicitudes de asilo en virtud del Reglamento Dublín II y facilitar la aplicación de este instrumento.

²⁶ El Plan de acción del programa de La Haya, citado, también se refiere al desarrollo de vínculos entre SIS II y el Sistema de información de Europol.

Vista la interrelación cada vez mayor entre sistemas de información desarrollados en el marco de la Unión Europea, que atañen a materias que se relacionan de manera clara con los objetivos del Tratado de Prüm, conviene hacer mención de forma específica al Sistema de Información de Schengen²⁷.

Es significativo que se haya denominado, aunque sea extraoficialmente al Tratado de Prüm como “Schengen III”, no sólo por la evidencia de que los siete Estados firmantes originarios del Tratado participan también en Schengen, sino por el hecho de compartir ámbitos de aplicación. Sin embargo, esta definición no es correcta, puesto que el intercambio de información a través de un instrumento jurídico ajeno al derecho de la Unión Europea, como es el Tratado, no debe considerarse como una fase más del Sistema de información de Schengen, que nace y se desarrolla en el marco jurídico propio de la Unión, y tiene unas finalidades y unas previsiones en cuanto a la protección de datos personales concretadas en su desarrollo normativo.

Actualmente se está desarrollando la nueva generación del Sistema de Información de Schengen (SIS II), a través de dos propuestas de Reglamento y una propuesta de Decisión²⁸. Estas propuestas, que conformarán la nueva definición del SIS II, han sido objeto de análisis y discusión en el Consejo y el Parlamento Europeo, lo que ha llevado a incorporar enmiendas a los textos originales²⁹.

Las propuestas afectan a materias del primer y del tercer pilar comunitario, puesto que se refieren básicamente a la inscripción de nacionales de terceros países en la lista de no admisibles, a efectos por tanto de denegación de entrada o estancia en el espacio Schengen; la descripción de personas buscadas para su detención y entrega o extradición; descripción

²⁷ Nos referimos al Convenio relativo a la supresión gradual de las fronteras comunes (Schengen, 14.6.1985) y al Convenio de Aplicación de los Acuerdos de Schengen (CAAS), de 19.6.1990. Respecto a España, ver: *Instrumento de Ratificación de 23 de julio de 1993 del Acuerdo de 25 de junio de 1991 de Adhesión del Reino de España al Convenio de Aplicación de 19 de junio de 1990 del Acuerdo Schengen de 14 de junio de 1985*.

²⁸ Propuesta de Decisión de Consejo relativa al establecimiento, funcionamiento y utilización del SIS II (COM (2005) 230); Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento, funcionamiento y utilización del SIS II (COM (2005) 236) y Propuesta de Reglamento del Parlamento y del Consejo relativo al acceso al SIS II por los servicios de los Estados miembros responsables de la expedición de los certificados de matriculación de vehículos (COM (2005) 237).

²⁹ Por lo que respecta a las tres propuestas, en fecha 25 de octubre de 2006 se ha realizado la primera lectura del texto en el Parlamento Europeo, a la que nos remitimos.

de personas con fines de protección o de prevención de amenazas; descripción de personas buscadas en el marco de procedimientos judiciales, y descripción de personas y objetos con fines de vigilancia discreta o de controles específicos, entre otras.

A los países que se incorporaron inicialmente al Convenio de Schengen (Alemania, Francia, Bélgica, Holanda y Luxemburgo), se añadieron otros (Italia en 1990, España y Portugal en 1991, Grecia en 1992, Austria en 1995, Dinamarca, Finlandia y Suecia en 1996, aunque Dinamarca mantiene un estatus especial). También se asociaron al CAAS Islandia y Noruega, aunque no son miembros de la UE, a través de un Acuerdo de asociación en 1999. Por su parte, Irlanda y Reino Unido no son parte integrante de los acuerdos, pero mantienen un estatus especial que se recoge en un protocolo del Convenio, y que implica la no vinculación de los dos Estados por determinados actos del acervo Schengen³⁰. Finalmente, en 2004 se establecen determinados acuerdos de colaboración con Suiza. Por tanto, los 18 países miembros participan de forma asimétrica en Schengen.

Con el SIS II se pretende la incorporación de los nuevos miembros de la UE desde 2004. Los ministros del Interior de los países de la UE, reunidos en Bruselas, han llegado al acuerdo sobre el calendario para el ingreso de estos países en el espacio Schengen. Concretamente, se prevé que la ampliación de Schengen se complete a partir de diciembre de 2007.

Como se ha avanzado, el SIS II apunta a cambios destacables en la arquitectura del sistema originario de intercambio de información de Schengen. El SIS consiste en un registro informatizado de datos relativos a personas y objetos (en relación éstos con vehículos u objetos buscados con finalidades de incautación o por constituir prueba en procedimientos penales), datos que se suministran y gestionan bajo la responsabilidad de los Estados miembros y que sirven para cumplir las finalidades del acervo Schengen.

El SIS por tanto tiene por objeto preservar el orden y la seguridad públicas, realizar control de fronteras y comprobaciones o controles de policía dentro del propio territorio, y velar por la aplicación de las disposiciones de Schengen que afectan a la circulación de personas por el territorio de los Estados miembros. En el ámbito de la inmigración, se aplica para controlar la lista de extranjeros “no admisibles” en el marco de la libre circulación de

³⁰ Se recuerda que a través del Tratado de Amsterdam, se adoptó un protocolo anexo al TUE y al TCE por el cual se integra el acervo Schengen al marco de la Unión Europea. El acervo comprende por tanto los dos Acuerdos citados, los protocolos de adhesión de los diferentes Estados miembros, así como las decisiones, declaraciones y actos adoptados posteriormente por el Comité Ejecutivo creado por el CAAS.

las personas (desarrollado por la propuesta de Reglamento correspondiente). Siendo esta materia propia del primer pilar comunitario, en cuanto a la protección de datos se aplica la Directiva 95/46/CE.

Por lo que respecta al resto de inscripciones previstas por el SIS II, que atañen a materias relativas al refuerzo de la cooperación policial y judicial en el ámbito penal (tercer pilar), en la propuesta de Decisión correspondiente de cita, en cuanto a la protección de datos, y como texto de referencia, el Convenio 108, del Consejo de Europa, de 1981. Sin embargo, hay que tener en cuenta la propuesta 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, comentada, que vendrá a sustituir determinados artículos de Schengen relativos a la protección de datos personales.

Ya se ha avanzado que el SIS II se está diseñando para permitir su ampliación a los nuevos países miembros de la UE, pero no es la única novedad. Se prevé la introducción de nuevas funcionalidades, en particular la posibilidad de interconexión de alertas y el uso de una plataforma técnica común entre SIS II y VIS. Se incrementa el número de las autoridades con acceso en el sistema, como Europol y Eurojust. Se introducen también nuevas categorías de datos, entre los que destacan los datos biométricos. El nuevo SIS, se desarrolla por tanto no ya como un instrumento de control de fronteras, sino como una más desarrollada herramienta de investigación³¹. Sobre la evolución del SIS II, destacan las opiniones que en reiteradas ocasiones ha emitido la Autoridad Común de Control de Schengen, en relación con la protección de datos personales³².

En conclusión es significativo destacar que la Unión Europea está planteando la posibilidad de incrementar la interrelación entre grandes sistemas de información europeos, en relación con la lucha contra la inmigración ilegal, y la lucha contra el terrorismo y la delincuencia organizada, esto es, los objetivos del Tratado de Prüm.

³¹ Sobre el desarrollo del SIS II, en relación con la protección de datos, ver el Dictamen del Supervisor Europeo de Protección de Datos, en *DOUE* serie C nº 91, de 19.4.2006.

³² La Autoridad Común de Control (ACC) de Schengen ha ido elaborando opiniones relativas al desarrollo del SIS II, a través de diversos documentos. En el más reciente, aprobado el 21 de septiembre por la ACC, se destaca la utilización de datos biométricos (huellas digitales) sólo a efectos de confirmación de identidad de nacionales de terceros países, entre otras valoraciones sobre el uso de datos biométricos en el SIS II.

Por su parte, el Grupo sobre Protección de Datos del Artículo 29 también ha recordado en su Dictamen 116/2005, de 25 de noviembre, la necesidad de concretar al máximo las finalidades del SIS II, los posibles accesos y el tratamiento de datos biométricos [ver: http://ec.europa.eu/justice_home/fsj/privacy].

Ello podría llevar a plantear una vez más un posible solapamiento de previsiones del Tratado de Prüm respecto a determinadas medidas que se están desarrollando dentro del entramado normativo del derecho de la Unión Europea. Por ello, como se apuntaba anteriormente, no deja de resultar engañosa la calificación del Tratado como un nuevo desarrollo del Sistema de información de Schengen. El Tratado de Prüm supone, por el contrario, un desarrollo paralelo de algunas de las finalidades de dichos sistemas de información, lo cual no contribuye a clarificar el marco normativo que, en cuanto a la protección de datos, debe tenerse en cuenta en los intercambios de información que el Tratado va a generar.

5. LAS PROPUESTAS DE DECISIÓN MARCO DEL CONSEJO RELATIVAS AL PRINCIPIO DE DISPONIBILIDAD Y A LA PROTECCIÓN DE DATOS EN EL TERCER PILAR COMUNITARIO

El Tratado de Prüm nace, como se ha apuntado, como un instrumento de colaboración intergubernamental entre siete países de la Unión fuera del marco institucional de la Unión Europea, con la finalidad de incrementar la seguridad a través del intercambio de información en relación con diversas materias, y supone una nueva aplicación del principio de disponibilidad de la información.

Como se ha avanzado, existen varias propuestas que afectarán de manera directa a la protección de datos. En concreto, las Decisiones marco que desarrollan el principio de disponibilidad y la protección de datos en el marco del tercer pilar comunitario van a tener que aplicarse por parte, entre otros, de los siete países firmantes del Tratado de Prüm. Como dispone el Tratado de la Unión Europea, las decisiones marco, sin efecto directo y de forma similar a las directivas europeas por lo que respecta a materias del primer pilar comunitario, obligan a los Estados miembros en cuanto al resultado, que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios.

5.1. *La propuesta de Decisión Marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad*³³

Puesto que ya se ha hecho mención extensa al principio de disponibilidad, en este punto destacaremos alguna previsión contenida en esta propuesta de Decisión marco.

³³ Al respecto, ver el Dictamen del Supervisor Europeo de Protección de Datos en *DOUE*, serie C, 116, de 17.5.2006.

Se autoriza el acceso a la información sólo a las autoridades nacionales competentes en materia de prevención, detección e investigación de delitos, obligando a las autoridades implicadas a que verifiquen la necesidad y la calidad de la información, y en este sentido se prevé que un comité específico verificará con carácter previo que la información sólo esté disponible para la autoridad competente equivalente (ver, en este sentido, en artículo 19 de la propuesta). Se prevé los Estados miembros adopten las medidas necesarias para ajustarse a las previsiones de la Decisión marco, en cualquier caso el 30 de junio de 2007 a más tardar.

Es destacable el hecho que esta propuesta se desarrolla de forma paralela a la propuesta que comentaremos más adelante, relativa a la protección de datos en el marco del tercer pilar. En concreto, se explicita que el refuerzo de las posibilidades de intercambiar información debe verse compensado por mecanismos de protección de los derechos fundamentales de la persona cuyos datos personales se tratan en virtud de la presente propuesta que desarrolla el principio de disponibilidad. Así, se prevé que la futura Decisión marco de protección de datos en el tercer pilar (por tanto, en el marco de la cooperación policial y judicial en materia penal) se aplicará a los tratamientos de datos efectuados por la propuesta de decisión marco que comentamos.

De alguna manera, pues, las dos propuestas de Decisión marco se complementan y se contrarrestan, ya que la primera facilita el intercambio de información en aplicación del principio de disponibilidad, y la segunda preverá medidas de protección de datos que serán aplicables al tratamiento de datos que se realice para el cumplimiento de las finalidades de cooperación policial y judicial en materia penal.

Volviendo a esta propuesta de Decisión marco relativa al intercambio de información en virtud del principio de disponibilidad, es destacable señalar que prevé un acceso en línea a la información (artículo 9), es decir, los Estados garantizarán que las autoridades equivalentes de otros Estados y Europol tengan acceso directo a la información contenida en determinadas bases de datos, así como una consulta en línea de datos índice (artículo 10) o acceso indirecto a estos datos índice, que remiten a la información que no está accesible en línea.

Por su parte, el anexo I de la propuesta define el contenido de la solicitud de información, mientras que el anexo II define los tipos de información que pueden obtenerse en virtud de la decisión marco con el fin de prevenir, detectar o investigar infracciones penales. En este sentido, se prevé que podrán obtenerse perfiles de ADN, es decir, los códigos alfanuméricos compuestos a partir de los marcadores del ADN del conjunto

de normas europeas (European Standard Set)³⁴, así como huellas dactilares, balística, información sobre matrículas de vehículos y datos mínimos que figuran en los registros civiles para la identificación de las personas, entre otros datos.

Todo ello, insistimos, siguiendo las normas que en lo que se refiere a la protección de datos, prevea la propuesta de Decisión marco que comentamos a continuación.

5.2. *La propuesta 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*

Esta propuesta³⁵ tiene por objeto garantizar la protección de datos personales en el marco de la cooperación policial y judicial, esto es, en lo que respecta al Título IV del TUE, correspondiente al tercer pilar comunitario, por tanto, puesto que en el tercer pilar comunitario no se aplica la Directiva 95/46/CE, esta Decisión Marco será su equivalente en el ámbito de cooperación policial y judicial.

La propuesta se refiere por tanto a datos personales que forman parte de un fichero gestionado por las autoridades competentes, a efectos de prevención y detección de infracciones penales, investigaciones y actuaciones judiciales en este ámbito, si bien la propuesta no se aplicaría al tratamiento de datos personales por la Oficina Europea de Policía (Europol), la Unidad Europea de Cooperación Judicial (Eurojust) ni el SIA (Sistema de Información Aduanera)³⁶.

Desde el momento en que entrase en vigor, a tenor de lo que dispone el propio Tratado en su artículo 47, esta Decisión marco afectaría al sistema

³⁴ Definidas en la Resolución del Consejo 2001/C 187/01, de 25 de junio de 2001, relativa al intercambio de resultados de análisis de ADN. La propuesta limita explícitamente el intercambio de datos de ADN a los perfiles de ADN.

³⁵ La referencia de la propuesta de Decisión marco es: 2005/0202(CNS). En relación con la misma propuesta, debe tenerse en cuenta el Informe del Parlamento Europeo de 18.5.2006, (A6-0192/2006), así como las enmiendas introducidas por el Parlamento Europeo en documento de fecha 14 de junio de 2006 (fecha del voto parcial del parlamento Europeo). Finalmente, en fecha 27 de septiembre de 2006, el Parlamento Europeo adoptó la correspondiente resolución legislativa.

³⁶ Respecto a este punto, la enmienda 7 al considerando 20 bis (nuevo) del Parlamento Europeo, (del citado documento) añadiría que estos tres sistemas de información “deben conservar aquellas de sus normas sobre la protección de datos que estipulan claramente que los datos personales sólo pueden tratarse, consultarse o transmitirse sobre la base de unas condiciones o restricciones más específicas y/o protectoras”.

de intercambio de datos de Prüm, resultándole aplicable. Sin embargo, habría que valorar en su momento el hecho de que ciertas previsiones del Tratado de Prüm resulten más específicas o garantistas respecto a la protección de datos personales, que la correspondiente Decisión marco³⁷.

Si bien nos remitimos al texto íntegro de la propuesta y a los documentos relacionados con ésta, conviene destacar a continuación algunas de las previsiones de la propuesta, que establece como punto de partida que los Estados miembros dispondrán que los datos personales únicamente puedan ser tratados por las autoridades competentes en virtud de una ley que establezca que el tratamiento es necesario para el cumplimiento de las funciones legales de la autoridad en cuestión, y con fines de prevención, investigación, detección y enjuiciamiento de delitos.

Destacamos, como parte del principio de calidad de los datos (artículo 4 de la propuesta), que los Estados miembros establecerán la obligación de distinguir claramente entre datos personales relativos a personas sospechosas de haber cometido o participado en un delito, o que hayan sido condenadas penalmente, o que se sospeche fundadamente que cometerá un delito, o que puedan ser testigos o víctimas de delitos, entre otras categorías³⁸.

Respecto a las categorías especiales de datos (artículo 6 de la propuesta), se parte de una prohibición inicial a su tratamiento, si bien ello no se aplicará si el tratamiento está previsto en una ley y es absolutamente necesario para la finalidad de prevenir, investigar, detectar o enjuiciar delitos, o consta el consentimiento explícito del interesado³⁹.

³⁷ En este sentido, ver: F. DEHOUSSE y D. SIFFLET: "Les nouvelles perspectives de la coopération de Schengen: Le traité de Prüm", disponible en <http://www.egmontinstitute.be/papers/06/eu/prum.pdf> [consulta 30 de julio, 2007], p.11.

³⁸ En las enmiendas del Parlamento Europeo relativas al principio de calidad de los datos, (enmiendas 12 a 16 del Parlamento) se añaden cuestiones relevantes como que los Estados miembros preverán la verificación periódica de la calidad de estos datos, la posibilidad del marcaje de datos en caso que el interesado niega que sean exactos, y tendrán en cuenta de forma específica las distintas categorías de datos personales (persona sospechosa, víctima, testigo, etc) y los fines para los cuales se recogen los datos.

³⁹ Resulta de interés la enmienda 21 del Parlamento Europeo (doc. cit.), respecto a los datos de ADN: Los Estados miembros preverán salvaguardas específicas adicionales en o que respecta a los datos biométricos y los perfiles de ADN, con el fin de garantizar que: Estos datos sólo se utilicen sobre la base de hechos comprobados y normas técnicas interoperativas; el nivel de exactitud de los datos biométricos y los perfiles de ADN se tenga cuidadosamente en cuenta y pueda ser refutado por el interesado por medios de fácil acceso; se asegure plenamente el respeto de la dignidad y la integridad de las personas.

En relación, todavía, con datos de ADN, ha habido en las dos propuestas de Decisión marco comentadas, consideraciones por parte del Supervisor Europeo de Protección de Datos.

Respecto a la puesta a disposición y transmisión de datos personales a las autoridades competentes de otros Estados miembros (artículos 8 y siguientes de la propuesta), se parte de que los datos sólo se transmitirán o se pondrán a disposición de las autoridades competentes de otros Estados miembros en caso necesario para el cumplimiento de las finalidades apuntadas de investigación de delitos, teniendo en cuenta criterios de control de calidad de los datos, artículo que también ha sido objeto de especial atención por el Parlamento Europeo, que ha añadido consideraciones respecto a la demostración por parte de los Estados del grado de necesidad de la transmisión de datos.

Tampoco se descarta la posibilidad de que se transmitan datos personales a autoridades competentes de terceros países o a organismos internacionales, si éstos garantizan un nivel adecuado de protección de datos y la transferencia es objeto de una obligación o autorización legal clara, previsión que también ha sido objeto de especial atención por parte del Parlamento Europeo en sus valoraciones sobre esta propuesta de Decisión marco.

La propuesta establece la creación de un grupo de protección de las personas en materia de protección de datos, de carácter consultivo, que constará de un representante de la Comisión, del Supervisor Europeo de Protección de Datos y de las autoridades de control de los Estados miembros (artículo 31)⁴⁰.

Los Estados miembros deberán garantizar que una o varias autoridades públicas independientes controlen la aplicación en su territorio de las previsiones de la Decisión marco, siendo las decisiones de estas autoridades independientes, y susceptibles de recurso jurisdiccional. También se prevé que deberá consultarse a estas autoridades de control para la elaboración de medidas reglamentarias o administrativas relativas a los derechos y libertades de las personas respecto al tratamiento de datos en materia penal (artículo 30 de la propuesta).

En la propuesta de Decisión marco de protección de datos en el tercer pilar, inicialmente no se explicitaba una referencia concreta a los datos biométricos y los perfiles de ADN. Sobre ello, el SEPD en su correspondiente Dictamen (consideración 79) recomienda que se prevean garantías específicas, entre otras, para asegurarse que sólo se utilicen datos biométricos y perfiles de ADN con arreglo a normas técnicas bien asentadas e interoperables; se tenga muy en cuenta su grado de precisión, y el interesado pueda impugnarlos por medios de fácil accesibilidad y se garantice plenamente el respeto de la dignidad de la persona.

⁴⁰ La enmienda 59 del Parlamento Europeo (doc. cit) añade que el Presidente del Grupo del Artículo 29 participará o estará representado en las reuniones del grupo. También se añade la previsión de una mayor participación del Supervisor Europeo de Protección de Datos, que sería consultado por el Grupo creado por la propuesta de Decisión marco.

En cuanto al ejercicio de los derechos de protección de datos, se prevé que el responsable del tratamiento de datos deberá proporcionar gratuitamente a la persona interesada información referida a la identidad del responsable, la finalidad y base jurídica del tratamiento, los destinatarios de los datos, entre otras informaciones. Además de esta obligación de información al interesado se prevén los derechos de acceso, rectificación, supresión o bloqueo (artículos 19 y siguientes).

Es destacable pues que, a través de las diversas enmiendas presentadas, el Parlamento Europeo propone una serie de puntualizaciones o añadidos al texto de la propuesta de Decisión marco.

Vista esta cuestión, no podemos dejar de hacer referencia, respecto a la propuesta de Decisión marco relativa a la protección de datos personales en el marco de la cooperación policial y judicial, al correspondiente Dictamen del Supervisor Europeo de Protección de Datos⁴¹. El SEPD destaca que la propuesta garantiza la aplicación en el ámbito del tercer pilar de los principios de protección de datos existentes en virtud de la Directiva 95/46/CE, puesto que la mayor parte de las disposiciones de la propuesta repiten las de otros instrumentos jurídicos de la Unión Europea en materia de protección de datos y son compatibles con dichos instrumentos. Por otra parte, considera que la propuesta aporta normas comunes que desarrollan estos principios, que en líneas generales resultan satisfactorias para proporcionar garantías adecuadas de protección de datos en el tercer pilar.

Debemos tener también en cuenta el Dictamen que las Autoridades Europeas de Protección de Datos han emitido en relación con esta propuesta de Decisión marco⁴². En este Dictamen se acoge positivamente la concreción de las medidas de protección de datos en el tercer pilar, y se destaca la importancia de conseguir un marco integral y coherente en la protección de datos personales en el ámbito de la cooperación policial y judicial. Por ello, consideran que las garantías previstas no sólo deberían aplicarse a aquellos datos transmitidos o recibidos de otro Estado miembro, sino a todo el conjunto de tratamientos de datos personales que, con esta finalidad, se llevan a cabo en todos los Estados miembros.

Finalmente, aparte de las dos propuestas de Decisión marco a las que hemos dedicado mayor atención, respecto a otras iniciativas en relación con el principio de disponibilidad que se están desarrollando actualmente

⁴¹ Publicado en el *DOUE* serie C 47, de 25.2.2006.

⁴² *Conference of European Data Protection Authorities. Opinion on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*. Brussels, 24 January 2006.

en la Unión Europea cabe citar también la Iniciativa del Reino de Suecia con vistas a la adopción de una Decisión marco sobre la simplificación del intercambio de información e inteligencia entre los cuerpos de seguridad de los Estados miembros de la Unión Europea, en particular en relación con delitos graves, incluidos los actos de terrorismo. Esta iniciativa, ha dado pie a la correspondiente propuesta de Decisión marco del Consejo, introduciendo cambios sustanciales en el redactado original⁴³.

El objetivo de esta propuesta, que ha dado pie a una adopción formal por el Consejo en fecha 18 de diciembre de 2006, es establecer normas en virtud de las cuales los cuerpos de seguridad de los Estados miembros puedan intercambiar de forma rápida y eficaz la información e inteligencia disponibles para llevar a cabo investigaciones penales u operaciones de información criminal, en particular en el caso de delitos graves. Por lo que respecta a la protección de datos personales, esta propuesta remite al 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, así como a los principios enunciados en la Recomendación (87)15 del Consejo de Europa dirigida a regular la utilización de datos de carácter personal en el sector de la policía, que según el artículo 8 de la propuesta de decisión marco deberán ser tenidos en cuenta en el correspondiente tratamiento de datos.

Así pues, en conclusión, vemos que el actual desarrollo a través de determinadas decisiones marco de la Unión Europea del principio de disponibilidad y de la protección de datos en el marco del tercer pilar comunitario, va a dar lugar a nuevas normas jurídicas que serán referente necesario para las previsiones del Tratado de Prüm, en cuanto al tratamiento de datos personales, en el momento en que sean normas vigentes. Todo ello, por aplicación del propio Tratado, en conexión con lo que dispone su artículo 47, ya citado, según el cual, las normas que en el futuro adopte la Unión Europea, y que puedan afectar al ámbito de aplicación del Tratado, in-

⁴³ Publicada en el *DOUE*, serie C, nº 281, de 18.11.2004. En relación con esta iniciativa, ver el proyecto de informe provisional del Parlamento Europeo, de 16.3.2005, con referencia 2004/0812 (CNS). En fecha 18.12.2006 se ha procedido a la adopción formal por el Consejo, que dará lugar a la correspondiente decisión marco del Consejo, documento 9827/06 de 2.10.2006. Por tanto, debe tenerse en cuenta la redacción final de dicha propuesta de decisión marco, respecto a los comentarios efectuados en este artículo. Respecto a ello, ver documentos con referencias: PRES/2006/349; CS/2006/16604; CS/2006/9827, en <http://ec.europa.eu/prelex/apcnet.cfm>. [Consulta 30 de julio, 2007].

cluyendo por tanto las previsiones relativas a la protección de datos personales, tendrían una aplicación prioritaria respecto a las previsiones del Tratado.

6. LA REMISIÓN AL DERECHO INTERNO EN EL TRATADO DE PRÜM

Las previsiones del Tratado de Prüm realizan una remisión continua al derecho interno, partiendo de que su artículo 1.1 dispone que el tratamiento de datos almacenados en ficheros de ADN se llevará a cabo con arreglo al derecho interno vigente para cada tipo de tratamiento; el artículo 5 del mismo añade que en caso de que se compruebe que existe concordancia entre perfiles de ADN por los procedimientos establecidos, la transmisión de otros datos de carácter personal disponibles relativos a los índices de referencia se efectuará con arreglo al derecho interno. Por su parte, el artículo 14, relativo a los fines de prevención de los delitos y amenazas para la seguridad en relación con grandes eventos de alcance transfronterizo, remite también a esta posibilidad “en la medida en que la transmisión de tales datos sea admisible con arreglo al derecho interno de la Parte Contratante transmitente”. Sin embargo, en éste y otros artículos (artículo 10, entre otros) se echa en falta una concreción mayor del tipo de datos relativos a persona que van a poder transmitirse. Finalmente, el artículo 47 prevé que las disposiciones del Tratado sólo serán aplicables en la medida en que sean compatibles con el derecho de la Unión Europea. Y añade que si en el futuro la UE adoptara normas que puedan afectar al ámbito de aplicación del Tratado, las disposiciones correspondientes del mismo dejarán de aplicarse en beneficio del derecho de la Unión Europea.

Todo ello indica que el marco normativo aplicable a los Estados parte del Tratado de Prüm (o Estados que en el futuro pudieran adherirse al mismo) quedan vinculados por lo que sea aplicable en el derecho interno en materia de protección de datos y por las normas que en esta materia adopte la Unión Europea.

Sin embargo, todo ello no está exento de problemas interpretativos y de encaje. Las normas que puedan aplicarse a los datos personales a raíz del Tratado de Prüm, pueden ser en este sentido de doble nivel. Por una parte, las normas específicas de protección de datos contempladas en el propio Tratado, y por otra parte, las normas que deban aplicarse, como derecho interno, esto es, las normativas estatales de protección de datos y las provenientes del entramado normativo que va creando la Unión Europea y que están, como hemos visto, en desarrollo.

Diversos autores⁴⁴ manifiestan en este sentido sus dudas sobre el encaje de las previsiones referidas especialmente a la protección de datos del Tratado de Prüm en el marco europeo, apuntando la idea de que el Tratado crea una jerarquía dentro de la Unión Europea, oponiéndose a la creencia generalizada que el nivel europeo debería ser predominante en los debates relativos a la seguridad. En este sentido, se estaría produciendo una ruptura política en la construcción del Área de libertad, seguridad y justicia de la Unión Europea⁴⁵.

Efectivamente, el Tratado remite de forma sistemática a la aplicación del derecho interno de cada país miembro en lo que respecta a la protección de datos personales. Así, por ejemplo, las consultas y transmisión de perfiles de ADN para su comparación, así como la transmisión de otros datos de carácter personal se regirán por el derecho interno de las partes, tal y como se concreta en los artículos 4 y 5 del Tratado, de la misma manera que la solicitud de una persona para que se examine la legalidad de un determinado tratamiento de datos o el derecho de las personas interesadas a la información e indemnización de daños, se regirán por el derecho interno del Estado en el que se hagan valer estos derechos, como se precisa en los artículos 39 y 40 del Tratado.

Por lo que respecta a España, habrá que remitirse a las previsiones que, en la legislación interna de protección de datos, sean aplicables a los tratamientos de datos derivados del Tratado de Prüm. En concreto, por la naturaleza de las bases de datos creadas a raíz del Tratado, tendremos que referirnos a lo que dispone el artículo 22 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, respecto a los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado, en conexión con lo que establece el artículo 2.2.c) de la misma ley⁴⁶.

⁴⁴ Estas y otras valoraciones se apuntan en: T. BALZACQ, D. BIGO, S. CARRERA y E. GUILD, "Security and the two-level game: The Treaty of Prüm and the management of threats". Centre for European Policy Studies (CEPS) *Working document*, nº 234, enero de 2006.

⁴⁵ T. BALZAC et al., op. cit. p. 2.

⁴⁶ La Ley Orgánica dispone en su artículo 2.2.c): "*El régimen de protección de datos de carácter personal que establece esta Ley Orgánica no es aplicable: (...) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada*". Por su parte, el artículo 22, citado, establece entre otras cuestiones, que "*La recogida y tratamiento para finalidades policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin el consentimiento de las personas afectadas están limitados a aquellos supuestos y aquellas categorías de datos que sean necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, y deben ser almacenados en ficheros específicos establecidos a tal efecto, que deben clasificarse por categorías en función del grado de fiabilidad*". (BOE núm. 298, de 14.12.1999).

Así pues, si bien existe la exigencia de compatibilidad con el derecho de la UE, la remisión al derecho interno podría comportar diferencias en el ejercicio de los derechos concretos de una persona frente al tratamiento de datos por aplicación del Tratado, en función del Estado miembro en que se realice el tratamiento, ya que entre las diferentes normas internas de protección de datos de cada país, podrían existir diferencias en este sentido, aunque se garantice el estándar mínimo que como hemos visto supone el Convenio del Consejo de Europa de 28 de enero de 1981.

En definitiva, la utilización de un instrumento ajeno al marco normativo surgido de la Unión Europea podría comportar la posibilidad de ciertos problemas de encaje de las previsiones del Tratado, en relación con el derecho fundamental a la protección de datos de carácter personal, tal y como se configura este derecho en el marco jurídico europeo o, cuanto menos, de ciertas dificultades de interpretación de las concretas normas aplicables al tratamiento de datos de carácter personal⁴⁷.

Si bien no es objeto de este artículo concretar el tratamiento de datos de ADN en el Tratado, es incuestionable que la gran novedad que supone la creación de este tipo de bases de datos, y la continua remisión que el Tratado hace al derecho interno, requiere hacer una breve mención del marco normativo a tener en cuenta en esta materia, más allá de lo que se ha apuntado anteriormente.

El Tratado de aplica a tipos específicos de información, en concreto, ADN, huellas dactilares y datos de matriculación de vehículos y establece la obligación concreta para los Estados de crear y mantener ficheros nacionales (sin especificar su número)⁴⁸ de análisis del ADN para los fines de la persecución de los delitos. Se establece pues que el tratamiento de datos en esos ficheros se llevará a cabo con arreglo al derecho interno vigente para cada tipo de tratamiento.

⁴⁷ En este sentido, algunos autores advierten que una de las cuestiones más delicadas que se plantean, son las posibles contradicciones del Tratado con el Derecho de la Unión Europea. Ver: F. DEHOUSSE y D. SIFFLET: "Les nouvelles perspectives de la coopération de Schengen: Le traité de Prüm", ya citado. En relación con el citado artículo 47 del Tratado, estos autores afirman que: "*Il faut toutefois déplorer que le traité ne spécifie rien à cet égard concernant les mesures d'application. Or, comme il présente un caractère largement programmatique, c'est surtout au niveau des accords d'application que les problèmes de compatibilité peuvent apparaître*". (pág. 9).

⁴⁸ El artículo 2.3 del Tratado dispone que en el momento del depósito de su instrumento de ratificación, aceptación o adhesión, cada Parte Contratante designará los ficheros nacionales de análisis de ADN a los que sean de aplicación las previsiones mencionadas en el Tratado.

En este sentido, puesto que el Tratado parte, por lo que respecta al tratamiento de los datos personales, de la compatibilidad con el derecho de la UE y remite a las previsiones del derecho interno, habrá que tener en cuenta la Resolución del Consejo, del 9 de junio de 1997, relativa al intercambio de los resultados de los análisis de ADN, así como la posterior Resolución del Consejo, de 25 de junio de 2001, relativa al intercambio de resultados de análisis de ADN. Dicha Resolución recoge la definición de algunos términos clave como “marcador de ADN”, “resultado de análisis de ADN”, “conjunto de normas europeas” o “marcador ESS («European Standard Set»)", definiciones que deben entenderse aplicables al tratamiento de datos generado por la entrada en vigor del Tratado⁴⁹.

Estas dos Recomendaciones parten de lo dispuesto en el Convenio del Consejo de Europa núm. 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Estrasburgo, 28 de enero de 1981), la Recomendación (87) 15 del Comité de Ministros del Consejo de Europa dirigida a regular la utilización de datos de carácter personal en el sector de la policía, y tienen en cuenta lo dispuesto en la Recomendación (92)1 de 10 de febrero de 1992 del Comité de Ministros del Consejo de Europa sobre la utilización de los resultados de análisis de ADN en el marco del sistema de justicia penal⁵⁰.

Si bien es cierto que a nivel interno los diferentes cuerpos de policía de los Estados firmantes utilizan bases de datos de ADN para finalidades de investigación policial, es un elemento de debate el hecho de que se haya podido o no ponderar suficientemente la necesidad y la proporcionalidad de la creación de nuevas bases de datos, dada la ausencia de participación de las instituciones de la Unión en el proceso que ha llevado al Tratado de Prüm⁵¹.

Debe tenerse en cuenta que, en los diferentes Estados firmantes del Tratado, ya existen diversas bases de datos con finalidades de investigación policial que contienen datos relativos al ADN, gestionados por los diferentes cuerpos de seguridad del Estado⁵².

⁴⁹ Ver *DOCE* serie C, nº 193, de 24.6.1997, y nº 187, de 3.7.2001, respectivamente.

⁵⁰ Los documentos del Consejo de Europa citados en este trabajo están disponibles en la página: <http://www.coe.int/legal/>

⁵¹ Sobre esta cuestión, ver: C.M. ROMEO CASABONA (Ed.), *Bases de datos de perfiles de ADN y criminalidad*. Cátedra Interuniversitaria, Fund. BBVA-Diputación Foral de Bizkaia de Derecho y Genoma Humano, Ed. Comares, Granada, 2002, p. 45 y ss.

⁵² A título de muestra, entre otros, el fichero “Fénix” de la Guardia Civil, que contiene el número de registro personal y perfil genético, en *BOE* nº 27, de 17.11.2004; el fichero “ADN-Veritas” del Cuerpo Nacional de Policía, que contiene vestigios biológicos y muestras para

A ello hay que añadir por lo que respecta a España, las previsiones del reciente Proyecto de Ley reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN⁵³. Nuevamente hay que apuntar la posibilidad de que se encuentren diferencias importantes en las normas equivalentes que en el derecho interno de otros Estados miembros del Tratado regulen las bases de datos de ADN.

7. CONCLUSIONES

La Unión Europea, en los últimos años, está avanzando en un progresivo intercambio de información, y por tanto, de datos personales, en relación con las materias que son objeto de tratamiento en el Tratado de Prüm, como son el terrorismo, la delincuencia transfronteriza y la migración ilegal. Este Tratado viene a ampliar las posibilidades del intercambio de información a través de un instrumento ajeno al derecho de la Unión Europea, diferente sustancialmente a otros grandes sistemas de información desarrollados por la Unión Europea, y por tanto puede resultar confuso definir el encaje que van a tener las diversas normas de protección de datos en los intercambios de información surgidos a raíz de la entrada en vigor del Tratado.

En este sentido hay que tener en cuenta que, más allá de que el Convenio del Consejo de Europa de 1981, en materia de protección de datos, sea un estándar mínimo de protección que los Estados miembros del tratado van a tener que considerar, el Tratado desarrolla el marco de la cooperación policial y judicial, y por tanto afecta a materias referidas al tercer pilar comunitario, respecto al cual todavía no existe una norma marco de protección de datos de carácter personal.

El Tratado de Prüm supone una nueva manifestación del principio de disponibilidad, desarrollado en diversas propuestas normativas de la Unión Europea, como las propuestas de Decisión marco sobre el intercambio de información en virtud del principio de disponibilidad y la propuesta de Decisión marco relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

cotejo, en *BOE* nº 165, de 11.7.2002; o el fichero "SIP IDENTISOS" de la policía de la Generalitat-mossos d'esquadra, que contiene perfiles genéticos, en *DOGC* nº 3694, de 7.8.2002.

⁵³ En diciembre de 2006 se aprueba por el Consejo de Ministros la remisión a las Cortes Generales del Proyecto de Ley reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. Sobre ello, ver la Proposición no *de ley* (nº 161/001714) sobre perfiles a partir del ADN. *BOCG* núm. 599 de 6.6.2006.

Va a ser fundamental, por tanto, el desarrollo de las normas que en el marco de la Unión Europea van a afectar a la protección de datos de carácter personal en materias referidas al tercer pilar comunitario, y que están desarrollando el principio de disponibilidad. En este sentido, y por aplicación de las disposiciones del propio Tratado, que exigen su compatibilidad con el derecho de la Unión Europea, con la entrada en vigor de las citadas normas, actualmente en desarrollo, éstas pasarán a formar parte del marco jurídico aplicable a las disposiciones del Tratado de Prüm en materia de protección de datos.

Sin embargo, en el momento actual estas normas marco todavía no son una realidad. En cuanto a la protección de datos de carácter personal, el Tratado de Prüm parte de sus propias previsiones, y de lo que disponga el derecho interno de cada Estado miembro. Con la entrada en vigor del Tratado, es el derecho interno el que deberá precisar determinadas cuestiones relativas al tratamiento de datos y a los derechos de los ciudadanos en relación con el mismo.

Efectivamente el Tratado remite, en aquello que no esté específicamente previsto en su articulado, al derecho interno, de manera sistemática. Esta remisión continua, en una materia tan específica como la utilización de bases de datos de ADN por parte de los Estados miembros del Tratado para el cumplimiento de las finalidades del mismo, implica tener en cuenta las diferencias que puedan surgir entre los diferentes modelos que establezca el derecho interno de cada Estado, por lo que respecta a estas bases de datos, y al tratamiento de éstos y otros datos de carácter personal a raíz de la entrada en vigor del Tratado.

El derecho interno va a tener que suplir las faltas de concreción del Tratado en algunos aspectos, como los referidos a detalles del ejercicio de derechos por parte del ciudadano, o la definición del tipo de datos personales que van a tratarse (artículos 10 y 14 del Tratado) entre otros. El derecho interno va a regular, en definitiva, y mientras no entren en vigor normas más específicas de protección de datos en el ámbito de la cooperación policial y judicial en materias del tercer pilar comunitario, el tratamiento y las comunicaciones de datos en el ámbito del Tratado, así como cuestiones relativas a la participación en el control de los tratamientos de datos por parte de las autoridades internas de protección de datos.

El hecho de que las previsiones de cada Estado en materia de ficheros policiales, de bases de datos de ADN y de protección de datos puedan ser diversas, no contribuye a dar claridad y homogeneización al tratamiento de datos de carácter personal en el ámbito del Tratado de Prüm. En este sentido, pueden darse diferencias entre las diversas leyes internas de pro-

tección de datos y entre las legislaciones nacionales que creen las bases de datos objeto de tratamiento en el Tratado de Prüm. Estas diferencias supondrían un menor riesgo para la seguridad jurídica, en concreto, para principios tan esenciales en materia de protección de datos como los principios de proporcionalidad y finalidad, si se contase con una suficiente armonización de las normas de protección de datos aplicables en el marco de la Unión Europea y por tanto, también, al Tratado de Prüm.

RESUMEN

La entrada en vigor del Tratado de Prüm va a afectar de forma importante a la protección de datos de carácter personal en diversos países de la Unión Europea. Para comprender cuál va a ser esta afectación, es necesario conocer el marco jurídico existente en la actualidad en la UE por lo que respecta a la protección de datos, y cómo se está desarrollando el principio de disponibilidad de la información en el marco europeo. En este sentido, vemos que todavía están en desarrollo varias normas que se aplicarán al tratamiento de datos personales en el ámbito del Tercer pilar de la UE, relativo a la cooperación policial y judicial en materia penal.

Además, el Tratado de Prüm remite sistemáticamente al derecho interno de cada Estado miembro, y a las previsiones de éste en materia de protección de datos. Más allá de que exista un estándar mínimo de protección en todos estos Estados, las diferencias entre las leyes internas de cada país podrían generar ciertas dificultades en cuanto al nivel efectivo de protección del ciudadano en relación con sus datos personales.

PALABRAS CLAVE: Tratado de Prüm, Primer y Tercer pilar en la Unión Europea, marco jurídico de la Unión Europea, Directivas y Decisiones Marco, protección de datos de carácter personal, Programa de La Haya, Principio de disponibilidad, el Sistema de Información de Schengen (SIS).

ABSTRACT

The entry into force of the Prüm Convention will have an important implication for the personal data protection in different states of the European Union. To understand this implication, it is necessary to know the current legal framework related to data protection in the EU, and how the EU is implementing the principle of availability of information in the European framework. In this context, it is evident that in the current moment, the EU is still developing several regulations that will be applied to the treatment of personal data in the ambit of the Third Pillar of the EU, related to police and judicial co-operation in criminal matters.

In addition, the Prüm Convention refers systematically to the domestic law of every member States, specifically in data protection matters. Even though it is clear that a standard minimum of data protection in all Member States exists, the differences between the domestic laws of every state could generate certain difficulties regarding the effective level of citizen protection in relation to their personal data.

KEY WORDS: Prüm Convention, The First Pillar and the Third Pillar in the European Union, European Union legal framework, Directives and Framework Decisions, the protection of personal data, the Hague Programme, the principle of availability, the Schengen Information System (SIS), Domestic Law.