EJERCICIO Y GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL CONVENIO DE PRÜM*

Emilio Aced Félez**

SUMARIO

1. INTRODUCCIÓN: EL PRINCIPIO DE DISPONIBILIDAD

Un elemento clave en el debate actual sobre la mejora de la cooperación policial entre los Estados miembros de la Unión Europea, al objeto de luchar contra el terrorismo y el crimen organizado, es el Principio de Disponibilidad. Dicho Principio se establece en el Programa de La Haya[1],

* Las opiniones vertidas en este trabajo representan exclusivamente el punto de vista del autor y no vinculan ni deben entenderse en ningún caso como la postura de ninguna institución u organización.

** Subdirector de Inspección de Datos y Tutela de los Derechos. Agencia de Protección de Datos de la Comunidad de Madrid. Ex-Presidente de la Autoridad Común de Control de Europol.

[1] Conclusiones de la Presidencia del Consejo Europeo celebrado en Bruselas los días 4 y 5 de noviembre de 2004. Se puede consultar en: http://ec.europa.eu/justice_home/news/

documento programático de la Unión Europea que define las prioridades en el ámbito de la seguridad en el periodo 2005-2010 con el fin de establecer un espacio europeo de justicia, libertad y seguridad. Este principio consiste en 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 puede obtenerla de otro Estado miembro. El organismo policial del otro Estado miembro que posea dicha información la facilitará para el propósito indicado, teniendo en cuenta los posibles requisitos de las investigaciones en curso en dicho Estado.

Como elementos adicionales y esenciales para la puesta en marcha del Principio de Disponibilidad, el Programa de La Haya señalaba los siguientes puntos:

a) El intercambio solamente puede tener lugar para la ejecución de tareas legales.

b) Debe garantizarse la integridad de los datos que deban intercambiarse.

c) Es necesario proteger las fuentes de información y garantizar la confidencialidad de los datos en todas las etapas del intercambio y ulteriormente.

d) Deben existir normas técnicas comunes para el acceso a los datos.

e) Debe supervisarse el respeto a la protección de los datos y garantizarse un adecuado control previo y posterior al intercambio de información.

f) Debe garantizarse la protección contra el uso indebido de los datos personales y el derecho a la corrección de los datos personales erróneos.

Además, el mencionado documento señalaba que «… Los métodos de intercambio de información 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 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 deberán crearse nuevas bases de datos europeas centralizadas sobre la base de estudios que hayan demostrado su valor añadido».

Pues bien, como veremos en los siguientes apartados, el sistema de

---

information_dossiers/the_hague_priorities/doc/hague_programme_es.pdf. Cfr. la Comunicación de la Comisión Europea al Consejo y al Parlamento del 19 de mayo de 2005 (COM (2005) 184 final): The Hague Programme: Ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice.

cooperación establecido en el Convenio de Prüm[2], tanto desde el punto de vista de su hincapié en el intercambio de determinada información de interés policial como por el uso intensivo de las tecnologías de la información y las comunicaciones para el acceso y diseminación de dicha información, se puede inscribir perfectamente –aún a pesar de no ser, jurídicamente hablando, un Convenio celebrado en el marco de la Unión Europea[3]– dentro de las iniciativas encaminadas a la efectiva implantación de dicho Prin-

[2] Tratado entre el Reino de Bélgica, la República Federal de Alemania, el Reino de España, 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, hecho en Prüm (República Federal Alemana) el 27 de mayo de 2005. Se puede consultar la versión española del mismo en el Boletín Oficial de las Cortes Generales, Sección Cortes Generales, VIII Legislatura, Número 230, de 17 de febrero de 2006, Serie A, bajo el epígrafe Actividades Parlamentarias. Se puede acceder a la versión en línea en el sitio web del Congreso de los Diputados (www.congreso.es).

[3] No obstante, en su preámbulo se establece expresamente que todas las Partes Contratantes son Estados de la UE. Además, el Convenio tiene una vocación expansiva y, en el segundo y tercer párrafos del preámbulo manifiesta claramente que las Partes firmantes del Convenio desean ofrecer *"... la posibilidad de participar en esta cooperación a todos los demás Estados miembros de la Unión Europea"* así como su deseo de *"...incorporar el régimen que establece el presente Tratado al marco jurídico de la Unión Europea, para conseguir una mejora al nivel de toda la Unión del intercambio de información, especialmente en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, creando a tal fin las bases jurídicas y técnicas necesarias"*.

Igualmente, en los apartados segundo y cuarto de su artículo 1 se afirma que esta cooperación *"... no afectará al derecho de la Unión Europea y, con arreglo al presente Tratado, estará abierta a la adhesión de cualquier Estado miembro de la Unión Europea"* y que *"...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 lo tanto, el objetivo final de los Estados signatarios del Convenio de Prüm sería la incorporación al mismo de todos los demás Estados de la UE así como la integración del mismo dentro del marco jurídico de la misma, lo que implicaría que el texto se convertiría en un nuevo Convenio intergubernamental de la Unión. En todo caso, aunque no todos los Estados miembros lleguen a formar parte del mismo y, por ello, no pudiera ser considerado como un Convenio de la UE, la inclusión del mismo en el entramado jurídico de la Unión podría llevarse a efecto a través del mecanismo de "cooperación reforzada" -que forma parte del Tratado de la UE desde la ratificación del Tratado de Ámsterdam y que fue reformado en el Tratado de Niza- ya que para que se reconozca dicha cooperación reforzada, es suficiente con que participen en la misma ocho Estados miembros y, en estos momentos, además de los siete Estados firmantes, otros como Eslovenia, Finlandia, Italia y Portugal, ya han manifestado su intención de adherirse al mismo.

cipio de Disponibilidad, habiéndose producido su génesis en paralelo con el desarrollo del mismo en el ámbito de la Unión.

Igualmente, en el párrafo cuarto del preámbulo del Convenio- adicionalmente a la manifestación de que los actos avalados por el mismo respetarán los derechos humanos tal y como se reconocen en la «Carta de los Derechos Fundamentales de la Unión Europea»[4], el «Convenio Europeo de Derechos Humanos y Libertades Fundamentales»[5] y las tradiciones constitucionales de los Estados participantes- se hace hincapié en particular en el apartado de protección de datos.

En concreto, se establece que el Estado receptor de la información debe garantizar un nivel de protección de datos adecuado (más adelante se examinará en qué términos) lo que, de nuevo, nos lleva a la necesidad de la existencia de un marco apropiado y armonizado de protección de datos en los Estados Parte del Convenio -de una manera muy similar a las condiciones que establecía el Programa de La Haya- para que los intercambios de datos personales que se lleven a efecto en base al Principio de Disponibilidad respeten las garantías esenciales relativas al derecho fundamental a la protección de datos personales, tal y como constan en los instrumentos jurídicos internacionales y nacionales antes mencionados.

Por ello, el análisis de las garantías en el ámbito de la protección de datos en el Convenio de Prüm también deberá abordarse teniendo en cuenta las condiciones inexcusables establecidas en el Programa de La Haya para que la implantación del Principio de Disponibilidad pueda considerarse legítima y proporcional.

2. LOS OBJETIVOS DEL CONVENIO DE PRÜM

La motivación y los objetivos fundamentales del Convenio de Prüm –también conocido como SIS III- se encuentran enunciados en el sucinto preámbulo que precede a su parte dispositiva. En efecto, el objetivo fundamental del Convenio es instituir una nueva medida compensatoria al espacio de libre circulación de las personas establecido en el Tratado de Schengen y en su Convenio de Aplicación[6], que forman parte del «acervo comunitario» desde la entrada en vigor del Tratado de Ámsterdam.

---

[4] DO Nº C 364, de 18 de diciembre de 2000, pp. 1 a 22.

[5] El texto del Convenio se encuentra disponible en la siguiente dirección: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=7&DF=11/27/2006&CL=ENG

[6] *DO Nº L 239, de 22 de septiembre de 2000. Todas las normas jurídicas de la Unión Europea se pueden consultar en EurLex (http://eur-lex.europa.eu/es/index.htm), el servicio de consulta jurídica en línea de la Unión Europea.*

En efecto, en el primer párrafo del preámbulo, se establece que en un espacio en el que las personas circulan libremente –logro conseguido en un primer momento al margen de las instituciones comunitarias y de la Unión Europea a pesar de ser dicha libertad de circulación uno de los principios esenciales de los Tratados– es cada vez más necesario que exista una mayor cooperación entre los Estados miembros para «…luchar con mayor eficacia contra el terrorismo, la delincuencia transfronteriza y la migración ilegal». Nótese que esta formulación expande de una manera incluso mucho más rotunda y abierta que los instrumentos legales relativos al Sistema de Información Schengen de segunda generación o SIS II –que se está debatiendo en estos momentos en las instituciones de la Unión Europea y cuya entrada en vigor se espera en 2007[7]– el objeto del Convenio de Schengen.

En efecto, en el Convenio de Schengen actualmente en vigor, el objetivo del Sistema de Información Schengen o SIS es, tal y como se enuncia en su artículo 92 «…el acceso a inscripciones de personas y objetos, al efectuar controles en la frontera y comprobaciones y otros controles de policía y de aduanas» así como (para la categoría de descripciones relativa a extranjeros a los que se les ha denegado la entrada en territorio Schengen, contemplada en el artículo 96) «…a efectos del procedimiento de expedición de visados, de expedición de permisos de residencia y de la administración de extranjeros».

Es decir, el SIS es un sistema de información del tipo conocido como «hit/no hit», esto es, su funcionamiento se basa en su utilización para la mera verificación de la existencia o no de información sobre una determi-

[7] Propuesta para una Decisión del Consejo sobre el establecimiento, operación y uso del Sistema de Información Schengen de segunda generación (SIS II), 31.5.2005, COM(2005) 230 final 2005/0103 (CNS); Reglamento del Parlamento Europeo y del Consejo sobre el establecimiento, operación y uso del Sistema de Información Schengen de segunda generación (SIS II), 31.5.2005, COM(2005) 236 final 2005/0106 (COD) y Propuesta para un Reglamento del Parlamento Europeo y del Consejo en relación con el acceso al Sistema de Información Schengen de Segunda Generación (SIS II) por parte de los servicios responsables de la matriculación de vehículos en los Estados miembros, 31.05.2005, COM(2005)237 final 2005/0104(COD). Todos ellos se pueden consultar en el sitio Web de la Comisión Europea http://ec.europa.eu/justice_home/doc_centre/police/schengen/doc_police_schengen_en.htm. En el sitio Web de la Organización No Gubernamental *Statewatch* (www.statewatch.org) se pueden consultar borradores más actuales de los textos internos que se están debatiendo en el Consejo.

En el sentido apuntado, cfr. la Decisión del Consejo: en el apartado segundo de su artículo 2, se establece que "…El SIS II contribuirá al mantenimiento de un alto nivel de seguridad dentro del área sin controles fronterizos de los Estados miembros", que ya amplía de una forma importante la prevista en el Convenio de Aplicación del Acuerdo de Schengen.

nada persona u objeto («alertas», en la terminología del SIS, término que ya ofrece una clara indicación del uso del sistema con una función de inmediatez y verificación rápida de hechos muy concretos y tasados en el Convenio de Schengen) sin que los datos obrantes en el mismo y su propia estructura permitan una utilización para finalidades policiales más amplias que aquéllas derivadas de la realización de determinados controles policiales y, en particular, controles de fronteras y aduaneros así como la vigilancia discreta o controles específicos sobre determinadas personas.

Por el contrario, el Convenio de Prüm tiene un objeto mucho más amplio que, como hemos visto, consiste en la lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, en el que ya no se menciona la mera realización de determinados controles sino que dicha formulación implica toda una declaración programática de utilizar los términos del Convenio para cualquier tarea policial, incluida la investigación criminal, que sirva a los fines enunciados más arriba.

En este sentido, no se puede dejar de mencionar que dicha formulación del objeto del Convenio puede abarcar cualquier tipo de delito por poco importante que sea siempre que el mismo tenga carácter transfronterizo –y en algunos casos aunque no lo tenga– pues ni siquiera se requiere como, por ejemplo, en el Convenio Europol, que la cooperación se refiera a «formas graves de delincuencia organizada» que afecten a dos o más Estados miembros. Y, especialmente, la colaboración preconizada por el Convenio de Prüm se encamina de manera muy específica al intercambio de información –en su mayor parte, datos de carácter personal– por lo que las garantías en el ámbito de la protección de datos personales deberían permitir una adecuada salvaguardia de este derecho fundamental de todas aquellas personas –sean ciudadanos europeos o no– cuyos datos van a tratarse en virtud de las previsiones del Convenio.

En los apartados siguientes analizaremos si estas salvaguardias existen en el articulado del Convenio y si garantizan el nivel adecuado de protección en relación con la sensibilidad de la información que se intercambiará y si respetan los requisitos establecidos en el Programa de La Haya para la puesta en marcha del Principio de Disponibilidad.

3. ELEMENTOS PRINCIPALES DEL CONVENIO DE PRÜM

El Convenio de Prüm se estructura en torno a ocho capítulos –Fundamentos del Convenio; Perfiles de ADN, datos dactiloscópicos y otros datos; Medidas para la prevención de atentados terroristas; Medidas para la lucha contra la migración ilegal; Otras formas de cooperación; Disposiciones

generales; Disposiciones Generales sobre protección de datos y Disposiciones de aplicación y disposiciones finales- que recogen los apartados más relevantes que regula el mismo. No obstante, se puede afirmar que los grandes temas en torno a los cuales gira el Convenio son el intercambio de datos genéticos, dactiloscópicos y sobre vehículos así como sobre determinadas personas sospechosas de causar disturbios públicos en eventos internacionales o de haber ejecutado o de planear atentados terroristas; las medidas de seguridad física tanto en el tráfico aéreo[8], en la lucha contra la falsificación de documentos públicos, los mecanismos de intervención conjunta y de actuación de agentes policiales en el territorio de otros Estados y, finalmente, las disposiciones generales en materia de protección de datos.

Dado el objetivo de este trabajo, el análisis se centrará en los aspectos relativos al primer y al último bloque, esto es, a las previsiones de los capítulos 2 y 7, que tratan, respectivamente, del régimen de intercambio de datos y las garantías de protección de datos establecidas en relación con dicho intercambio.

4. EL INTERCAMBIO DE DATOS

El capítulo 2 describe los intercambios de datos entre las partes regulados por el Convenio. Este intercambio incluye tanto datos personales como no personales, aunque prácticamente la totalidad de datos intercambiados tienen la consideración de personales. En concreto, se instituyen mecanismos de intercambio de datos genéticos, dactiloscópicos, de registro de vehículos y los relativos a las medidas de seguridad en grandes eventos transfronterizos.

El Convenio comienza el capítulo estableciendo el compromiso para todas las Partes de crear bases de datos nacionales de análisis de ADN con la finalidad de persecución de los delitos, que se regularán de acuerdo con el derecho interno de cada Estado sin perjuicio de las propias disposiciones del Convenio.

A continuación, se implanta la obligación de cada Parte de disponer de índices de referencia relativos a la información contenida en los ficheros antes mencionados. Dichos índices deberán contener exclusivamente perfiles de ADN obtenidos de la parte no codificante[9] de dicho ADN y una

[8] Los llamados “sky marshalls” o funcionarios de policía presentes en determinados vuelos y su régimen jurídico y de transporte y utilización de armas.

[9] Es decir, secuencias de ADN que no parecen contener genes y que se utilizan exclusivamente como mecanismo de identificación sin que, en el estado actual de la ciencia, puede deducirse de ellos ningún otro tipo de información genética, como la relativa a posibles enfermedades actuales o futuras.

referencia, de tal manera que la consulta de los mismos no permita identificar «directamente» a la persona concernida.

Igualmente, aquellos índices de referencia que no puedan atribuirse a ninguna persona –por ejemplo, aquéllos hallados en el lugar de comisión de un crimen pero de los que se desconoce a qué persona pertenecen– o «huellas abiertas», deberán hacerse constar como tales en la lista de índices de referencia. Los índices de cada Parte deberán poder ser consultados de forma automática por el resto de Estados participantes en el Convenio.

En relación con la consulta de estos índices de referencia, el Convenio instaura –siguiendo una metodología que se repite en todas las distintas secciones o áreas temáticas del mismo– la obligatoriedad de que la misma se realice a través de los llamados «puntos de contacto nacionales».

Estos puntos de contacto nacionales tendrán acceso al resto de índices de referencia para una finalidad tan amplia como la enunciada en el apartado primero del artículo 3: la persecución de delitos. Nótese una vez más como, respecto del principio de finalidad, el Convenio no establece ninguna restricción en la posibilidad de consulta de los índices de referencia de todas las Partes del Convenio en función de la gravedad del delito investigado o de la posible pena asociado al mismo. Tampoco se exige que el delito afecte a más de un Estado parte del Convenio por lo que, en la práctica, la consulta a estos datos genéticos podría llevarse a cabo –aunque en buena lógica no será la praxis habitual– en el transcurso de una investigación penal sobre delitos de poca importancia o relevancia.

La única restricción que aparece en el mismo apartado primero es que las consultas deberán llevarse a cabo en relación con «casos concretos», esto es, se excluye la legalidad de búsquedas genéricas en los índices de referencia sin que exista una necesidad demostrable para un caso concreto y de acuerdo con lo que establezca el derecho nacional.

Estos aspectos abren un debate, que aparecerá en otros puntos de este documento, sobre la proporcionalidad de estas medidas y si realmente la posible intrusión en la privacidad de las personas que las mismas suponen se encuentra equilibrada en todos los casos con un importante beneficio para el interés general y sobre si las mismas constituyen una medida necesaria en el ámbito de una sociedad democrática, tal y como dispone el artículo 8 del Convenio Europeo de Derechos Humanos.

Si en un proceso de consulta se obtiene una coincidencia con una referencia existente en otro Estado Parte, se informará de ello a la Parte

consultante que, en ese caso, tendrá derecho a que se le remitan otros datos de carácter personal asociados a la referencia de que se trate, siempre con arreglo a lo que disponga el derecho interno de la Parte consultada y en concordancia con lo establecido en el artículo 15, es decir, a través de los puntos nacionales de contacto ya mencionados. Al instituir el Convenio la obligatoriedad de estos puntos nacionales prácticamente en todas las áreas de cooperación que contempla, los trataremos conjuntamente más adelante.

En este apartado conviene detenerse para plantear una cuestión de capital importancia que afecta tanto a los índices de referencia de perfiles de ADN como de datos dactiloscópicos. En efecto, en el párrafo segundo del artículo 2 y en el artículo 8 se afirma que los índices de referencia «… no podrán contener datos que permitan identificar directamente a la persona concernida».

¿Significa esto que para el legislador los datos contenidos en los índices de referencia no tienen la consideración de datos de carácter personal? Para responder a esta pregunta no es suficiente con consultar la definición de «tratamiento de datos de carácter personal» que aparece en el artículo 33 del Convenio, dentro del capítulo 7, dedicado a las Disposiciones generales sobre protección de datos, ya que la misma, aun detallando meticulosamente aquellas operaciones que pueden ser consideradas tratamiento de datos personales, no ofrece ninguna pista para determinar lo que, a efectos de la aplicación del Convenio de Prüm, pueden considerarse datos de carácter personal.

Así pues, para su determinación no existe otra solución que acudir a los instrumentos jurídicos que, a tenor de lo dispuesto en el artículo 34, habrán de regir como norma de mínimos en relación con el tratamiento de datos personales en los Estados Parte del mismo. Así, el mencionado artículo 34 instaura como requisito inexcusable –siguiendo en ello a todos los Convenios y Decisiones de la Unión Europea en materia de cooperación policial y judicial- para que un Estado pueda ser Parte del mismo, el que tenga efectivamente implantadas las garantías presentes en el «Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal o Convenio 108» y su «Protocolo Adicional de 8 de noviembre de 2001 sobre autoridades de control y flujos transfronterizos de datos» (por cierto, todavía ni firmado ni ratificado por España, aunque todos sus elementos forman parte de nuestra legislación de protección de datos) y en consonancia con la «Recomendación (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»[10]. El Convenio de Prüm obliga a que estas reglas mínimas se apliquen también cuando los datos son objeto de tratamiento no automatizado.

Pues bien, el Convenio 108 define datos de carácter personal como «… cualquier información relativa a una persona física identificada o «identificable». Por su parte, aun cuando 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»[11], no resulta aplicable directamente a los tratamientos policiales -aunque muchos Estados de la Unión Europea no los hayan excluido del ámbito de aplicación de la ley que la transpone a su ordenamiento interno- define datos personales como «…toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya «identidad pueda determinarse, directa o indirectamente», en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

Finalmente, la «Propuesta de la Comisión Europea para una Decisión Marco del Consejo sobre la protección de los datos personales tratados en el marco de la cooperación policial y judicial» (en adelante, la Decisión Marco)[12], que está llamada, una vez aprobada, a sustituir al Convenio 108 como norma de referencia en materia de protección de datos en el ámbito de la cooperación policial y judicial dentro de la Unión Europea, repite milimétricamente la definición de la Directiva 95/46/CE antes reproducida.

Por lo tanto, si hemos de atender a las definiciones estándares de los textos legales a los que el Convenio se refiere o a aquellos otros que establecen el estándar de protección de datos en la Unión Europea, es evidente que en todos ellos se parte de la base de que la mera posibilidad de identificar a una persona a través de un conjunto de datos, aunque dicha relación de identidad «no sea directa», es suficiente para considerar que los datos considerados han de ser clasificados en la categoría de datos personales.

Así pues, en primer lugar, aun excluyendo que se pueda utilizar la información de perfiles de ADN presente en los índices de referencia en

---

[10] La regulación sobre protección de datos del Consejo de Europa se puede consultar en http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/

[11] DO Nº L 281, de 23 de noviembre, pp. 31 a 50.

[12] COM (2005) 475 final, de 4 de octubre de 2005.

sentido inverso al previsto en el Convenio, esto es, cruzando dicho perfil con los existentes en las bases de datos nacionales, lo que podría proporcionar en algún caso una identificación directa; el nexo directo e inmediato entre la referencia contenida en el índice y la de la base de datos nacional de la que forma parte el perfil de ADN que se publica para su consulta por las otras partes, excluye la posible aplicación, siquiera a efectos interpretativos, de lo que establece el Considerando 26 de la Directiva de Protección de Datos «… (26) Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona…», ya que, como se ha mencionado, el establecimiento de la conexión entre la referencia y la identidad de la persona tan sólo requiere una consulta a la base de datos nacional de la que procede el perfil.

Por todo ello, no cabe ninguna duda de que los índices de referencia, tanto de ADN como de datos dactiloscópicos, contienen «datos de carácter personal» y, por ello, están amparados por todas las garantías de protección de datos aplicables a los tratamientos de datos personales previstos por el Convenio. No obstante, por mor de la claridad y la seguridad jurídica, este aspecto de capital importancia debería clarificarse en el Acuerdo de Ejecución previsto en el Convenio, sobre todo a resultas del poco afortunado epígrafe que encabeza el artículo 14 «Transmisión de datos de carácter personal», que parece dar a entender que el resto de los datos cuyo intercambio instaura el Convenio no tendrían la calificación de personales.

Además del procedimiento general descrito, existen otros dos aspectos más específicos que son abordados en los artículos 4 y 7 bajo las rúbricas «Comparación automatizada de perfiles de ADN» y «Obtención de material genético molecular y transmisión de perfiles de ADN».

En el primer caso, se trata de la instauración de un procedimiento automatizado para verificar todas las «huellas abiertas» de cada Parte contra los índices de referencia del resto de Estados al objeto de intentar la identificación de los mismos en las bases de datos de otro Estado en el que pudiera constar la identidad. La transmisión y comparación se llevará a cabo de forma automatizada y solamente si la legislación nacional de las Partes lo permite.

Por su parte, el artículo 7 regula la obtención de material genético de una persona residente en un Estado Parte del Convenio distinto de aquel en que se lleva a cabo una investigación que requiera la obtención del

mismo. La Parte requerida deberá prestar asistencia judicial mediante la obtención y análisis del material genético molecular de la persona requerida, siempre y cuando la Parte requirente comunique la finalidad para la que se solicita el material genético y se cumplan los requisitos legales previstos para la obtención de dicha muestra en el derecho nacional tanto de la Parte requirente como de la Parte requerida.

Las previsiones para datos dactiloscópicos establecidas en los artículos 8 a 12 son similares a las analizadas para los datos de perfiles de ADN –con la diferencia que no se establece la obligatoriedad de creación de nuevas bases de datos sino de «poner a disposición» del resto de las Partes las bases de datos dactiloscópicas existentes– y por ello no nos detendremos de nuevo en ellas, pues les son de aplicación los mismos comentarios realizados en los párrafos anteriores. Simplemente, ha de notarse que el legislador no ha previsto para el caso de las huellas dactilares la posibilidad de una comparación automatizada de aquellas que podrían considerarse, siguiendo la nomenclatura utilizada para los perfiles de ADN, «abiertas» o que aún no se conoce a quién pertenecen, para intentar establecer la identidad de su propietario.

A continuación, en el artículo 12, se regula la consulta de los datos obrantes en los registros de vehículos de los Estados Parte del Convenio. En este caso no se establece la creación de índices de referencia intermedios, sino que se avala la consulta directa y automatizada de dichos registros. A través de dicha consulta –que sólo se podrá llevar a cabo si se cuenta con los datos completos de matrícula o del código de identificación del vehículo para evitar lo que en los países de lengua inglesa se conoce como «fishing expeditions»– se podrán conocer «datos sobre los propietarios o usuarios[13] del vehículo» y «datos sobre el vehículo», utilizando expresiones indefinidas que no permiten evaluar la necesidad y proporcionalidad de la información suministrada al resto de las Partes.

Además, hay un aspecto especialmente relevante en el primer apartado del artículo 12 que merece un comentario aparte. El tenor literal del mismo dispone que «… Las Partes Contratantes permitirán que los puntos de

[13] La inclusión de los datos de usuarios de los vehículos como datos que pueden extraerse de los registros de matriculación es bastante sorprendente, ya que no hay ningún registro de vehículos (al menos en España) que contenga datos de los posibles usuarios de los mismos, sino únicamente de sus propietarios. Si se facilitan datos de usuarios, es evidente que los mismos no provendrán de los ficheros de matriculación, sino de otras fuentes y no serán obtenidos mediante la consulta a estas bases de datos, por lo que no se entiende bien que figuren en este epígrafe.

contacto nacionales de las demás Partes Contratantes mencionados en el apartado 2, para los fines de la prevención y persecución de delitos y de la «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 para la prevención de amenazas para la seguridad y el orden público, tengan acceso a los (…) datos contenidos en los registros nacionales de vehículos, con derecho a consultarlos de forma automatizada en casos concretos».

La frase resaltada introduce un elemento de inseguridad al no concretar exactamente a qué tipos de infracciones se está refiriendo. La formulación elegida parece omnicomprensiva puesto que cualquier persona sancionada por cualquier tipo de infracción administrativa-independientemente de la competencia directa y evidente de la fiscalía y los tribunales para la persecución y enjuiciamiento de los ilícitos penales– tiene derecho a acudir a los tribunales de justicia para obtener amparo si está disconforme con una resolución administrativa o cree que sus derechos no han sido respetados.

No obstante, el objeto general de Convenio ya analizado, esto es, intensificar la «… cooperación para luchar con mayor eficacia contra el terrorismo, la delincuencia transfronteriza y la migración ilegal», no parece avalar una interpretación tan extensiva. Así pues, dicha cláusula debería entenderse como circunscrita a las infracciones sobre las cuales el Convenio establece algún tipo de medida o instaura intercambios de información.

Ello incluiría la investigación y persecución de delitos en los términos contemplados en el Convenio (de forma muy extensiva por cierto, como ya se ha indicado) y aquellas infracciones conectadas con los vehículos o los eventos transfronterizos mencionados en el artículo 14. Sin embargo, sería conveniente que en el Acuerdo de Ejecución se determinara de forma clara y precisa el verdadero alcance de este punto por su importante repercusión en el derecho a la protección de datos de las personas.

El siguiente aspecto que trata el Convenio en el cual los datos personales son relevantes es, precisamente, el artículo 14 que, como ya se mencionó con anterioridad, ostenta el título, no especialmente afortunado, de «Transmisión de datos de carácter personal». En realidad, se refiere a la transmisión de datos relativos a personas «… 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…».

Estas transferencias de datos se llevarán a cabo en relación con la celebración de eventos de alcance transfronterizo y, en particular, en el terreno de los acontecimientos deportivos y en el de las celebraciones del

Consejo Europeo. El artículo 14 no especifica qué tipo de información –a petición de otra Parte o por iniciativa propia- se intercambiarán las Partes, lo que deja un amplísimo margen de discrecionalidad a las autoridades competentes para decidir qué información se comparte.

Ello es todavía más cierto si se pone en relación con las causas que pueden motivar el intercambio de información y que, además de condenas firmes previas, incluyen la existencia de «otras circunstancias» que permitan suponer que las personas cuyos datos se comparten van a cometer un delito con motivo de la celebración del evento de que se trate. Como se puede observar, el margen de apreciación que pueden utilizar las autoridades competentes es enorme y, expresado en román paladino, viene a significar que se pueden intercambiar prácticamente cualquier tipo de datos por cualquier causa o sospecha, lo que no parece resultar compatible con una sana implantación de los principios de protección de datos

Por ello, el Acuerdo de Ejecución debería de circunscribir la interpretación de este precepto a sus justos términos y dar una clara indicación de las personas y datos que pueden verse afectados por la aplicación de este artículo y, de ese modo, contribuir a la predictibilidad de la aplicación de las normas jurídicas reiterada en tantas ocasiones por el Tribunal Europeo de Derechos Humanos como un componente cardinal de toda regulación respetuosa con el Convenio Europeo de Derechos Humanos y Libertades Fundamentales.

En cualquier caso y hasta que se disponga de la relación de datos transferibles, la enumeración de posible tipos de información que se pueden remitir desde una Parte a otra Parte a requerimiento de esta última en situaciones de cooperación en el caso de celebración de grandes acontecimientos, catástrofes o accidentes graves y que aparece detallada en el apartado segundo del artículo 27 podría servir como guía a la hora de definir de una manera algo más precisa el tipo de datos que se pueden intercambiar, ya que se refiere a situaciones similares a las contempladas en el artículo 14.

Por el contrario, en el aspecto relativo a la retención de datos, el Convenio se muestra mucho más claro y explícito al establecer que los mismos deberán de ser suprimidos inmediatamente «… cuando se hayan cumplido los fines (…) «para los que se transmitieron»» o «…cuando ya no puedan cumplirse», formulación que sigue la doctrina clásica establecida en tantas normas de protección de datos cuando se trata de la proporcionalidad del tratamiento en relación con la finalidad que lo justifica.

No obstante, y por si en algún caso la regla general no proporciona una guía suficiente para decidir sobre la supresión de los datos personales

transmitidos en función de lo establecido en dicho artículo, el Convenio dispone taxativamente que el plazo máximo de conservación de los datos será, en todo caso, de un año, previsión a la que la única crítica que cabría hacerle es que quizás se trate de un plazo excesivamente largo dado el carácter puntual y sumamente limitado en el tiempo de la situación que justifica la transmisión de los datos de carácter personal, salvedad hecha, claro está, de aquellos datos que hayan sido utilizados con posterioridad por las autoridades policiales o judiciales en investigaciones concretas o procedimientos judiciales.

Finalmente, para concluir el apartado dedicado a la regulación de los intercambios de datos, en el artículo 15, primero del capítulo tercero dedicado a las «Medidas para la prevención de atentados terroristas» se contempla una nueva posibilidad de transmisión de información con el objeto de prevenir estos atentados. Se trata de la posibilidad existente de transmitir, conforme a las disposiciones del derecho nacional de la parte remitente, determinados datos e informaciones, que se detallan en el apartado segundo, «… porque determinados hechos justifiquen la presunción de que las personas de que se trate van a cometer delitos según lo dispuesto en los artículos 1 a 3 de la Decisión Marco nº 2002/475/JAI del Consejo de la Unión Europea, de 13 de junio de 2002, para la lucha contra el terrorismo»[14].

Estos datos –que consistirán en el nombre, apellidos, fecha y lugar de nacimiento, así como la descripción de los hechos que justifican la presunción mencionada en el apartado primero– se podrán transferir a iniciativa propia, sin necesidad de que medie requerimiento de la Parte destinataria de la información. La Parte remitente puede estipular, de acuerdo con su derecho nacional, determinadas condiciones para la utilización de los datos que remite. Estas condiciones serán vinculantes para la Parte receptora de la información.

Nos encontramos otra vez ante una transmisión de datos prevista en el Convenio que adolece de una gran indeterminación. Todos estaremos de acuerdo en que la lucha contra el terrorismo, más que ningún otro motivo, justifica una rápida, ágil y eficaz colaboración entre los servicios policiales de los distintos Estados, pero la formulación de dicha cooperación de una manera tan vaga, podría suponer la vulneración de los derechos de las personas ya que, por ejemplo, no existe ninguna manera de saber cuáles serán esos «hechos que justifiquen la presunción» de que una determinada

[14] DO Nº L 164, de 22 de junio de 2002, pp. 3 a 7.

persona va a cometer un delito y ello podría entrañar que la aplicación del Convenio carezca de los elementos necesarios para saber, con una cierta certidumbre, cuáles serán las conductas o los sucesos que justifican la transferencia de datos de una persona.

Así pues, sería conveniente que en el Acuerdo de Ejecución, siquiera a modo de ejemplo y sin necesidad de que se considere una lista cerrada y exhaustiva, se indicaran los hechos principales, más frecuentes o más importantes que podrían justificar la transmisión de datos personales que estamos analizando.

No olvidemos que dicha transmisión de datos puede tener consecuencias muy graves para las personas de que se trate y que una mera sospecha o información difusa no puede justificar la categorización de un ciudadano como un posible terrorista. Esto es aún más cierto desde el momento de que en este apartado no existe ninguna previsión que limite los periodos de tiempo durante los cuales estas informaciones permanecerán en las bases de datos del Estado de destino de la misma.

5. LOS PUNTOS NACIONALES DE CONTACTO

A lo largo de todo el articulado del Convenio y siguiendo la técnica de otros instrumentos internacionales de cooperación policial, se establece que los intercambios de información se llevarán a cabo a través de unidades concretas y especializadas de cada Estado Parte del Convenio. A estas unidades se las denomina «puntos nacionales de contacto». Su establecimiento sirve al propósito de organizar los intercambios de información en torno a unidades con un conocimiento cabal de las normas del Convenio y de los requisitos que las peticiones y respuestas deben cumplir al tiempo que al establecimiento de interlocutores claros y conocidos por todos los Estados participantes.

Desde el punto de vista de la protección de datos personales, su designación no puede ser sino bienvenida pues suponen un filtro necesario para el encaminamiento de los intercambios de datos personales y contribuyen a que la diseminación de la información se lleve a cabo de una forma ordenada y controlada.

Por otra parte, la centralización de la gestión de los intercambios en los mismos debe llevar aparejada la debida formación de sus miembros así como la adopción de importantes medidas de seguridad que impidan el acceso o utilización no autorizado de la información que custodian.

Dado que las previsiones del Convenio abarcan campos muy diferentes

de la actividad policial y para poder adaptarlas a los distintos modelos policiales de los Estados Parte, se ha optado por la posibilidad de establecer puntos nacionales de contacto por cada una de las actividades recogidas en el Convenio en lugar de definir, de forma obligatoria, un único punto de contacto encargado de gestionar todos las actividades de cooperación que el mismo establece[15]. Con ello se dota de la suficiente flexibilidad a los Estados en los cuales las distintas competencias pudieran estar repartidas en autoridades diferentes y que, por ello, pudiera resultarles adecuado distribuir el control sobre los intercambios en unidades diferentes aunque, en general, no es de esperar una proliferación excesiva de puntos nacionales de contacto.

La regulación de los mismos es homogénea a través de todo el Convenio y las competencias de todos los puntos nacionales de contacto que se mencionan en el mismo[16] se rigen por lo previsto en el derecho nacional de cada una de las Partes.

No obstante, existe una diferencia entre las disposiciones que se refieren a los puntos de contacto nacionales previstos en los artículos 6, 11 y 12. Respecto de éstos, dada la necesidad de establecer mecanismos técnicos de interconexión y comunicación de los índices de referencia y de los registros de vehículos, se dispone que los detalles y pormenores técnicos se definirán en un Acuerdo de Ejecución, tal y como se prescribe en el artículo 44, que prevé la posibilidad de que las Partes celebren acuerdos sobre la base del Convenio y en el marco del mismo, para su ejecución administrativa.

---

[15] Aunque en el caso español se ha optado precisamente por designar un único punto de contacto tal y como se puede comprobar en la Declaración formulada por el Reino de España en el momento de la ratificación del Convenio, que designa a la Secretaría de Estado de Seguridad del Ministerio del Interior como punto de contacto nacional a todos los efectos.

[16] Con arreglo al *apartado primero del artículo 6*, los puntos nacionales de contacto para los análisis del ADN; con arreglo al *apartado segundo del artículo 11*, los puntos nacionales de contacto para los datos dactiloscópicos; con arreglo al *apartado segundo del artículo 12*, los puntos nacionales de contacto para los datos de los registros de vehículos; con arreglo al *artículo 15,* los puntos nacionales de contacto para el intercambio de información relativa a grandes eventos; con arreglo al *apartado tercero del artículo 16*, los puntos nacionales de contacto para las informaciones relativas a la prevención de atentados terroristas; con arreglo al *artículo 19*, los puntos nacionales de contacto y de coordinación para los escoltas de seguridad de los vuelos; con arreglo al *artículo 22*, los puntos nacionales de contacto y de coordinación para los asesores en materia de documentos; con arreglo al *apartado tercero del artículo 23*, los puntos nacionales de contacto para la planificación y ejecución de las repatriaciones.

6. LAS DISPOSICIONES GENERALES SOBRE PROTECCIÓN DE DATOS

Abordamos ahora la regulación propiamente dicha de la protección de datos en el Convenio que se establece en su capítulo séptimo. El capítulo comienza con una serie de definiciones encabezada por el concepto de tratamiento de datos personales sobre la que en principio no hay nada que objetar, salvo que se haya optado por innovar cuando existen definiciones generalmente aceptadas de tratamiento de datos personales, como la de la Directiva 95/46/CE.

No obstante, hay dos aspectos que merecen resaltarse. El primero de ellos es que la definición de tratamiento se extiende tanto a tratamientos manuales como automatizados, lo que anticipa la aplicación a ambos tipos de tratamiento de las normas marco de protección de datos que el Convenio invoca y a las que ya se ha hecho referencia con anterioridad.

El segundo de ellos es la consideración explícita como tratamiento de datos personales de la comunicación de la existencia o inexistencia de una concordancia respecto de los argumentos utilizados en una consulta o en una comparación, tal y como se definen en el Convenio.

Esta clarificación, aunque la existencia de un tratamiento de datos personales se desprende de la argumentación realizada en el apartado cuarto de este trabajo en relación con la categorización de los índices de referencia como datos personales, siempre es bienvenida y evita posibles interpretaciones dispares.

De todas formas, la inclusión de la definición de tratamiento de datos personales no hace sino resaltar la carencia de definición del concepto de «datos de carácter personal». Los argumentos a favor y en contra de incluir este tipo de definiciones de conceptos básicos en una regulación legal son idénticos para ambos conceptos y habría sido de desear mayor coherencia a la hora de decidir la inclusión o ausencia de ambos.

Se definen a continuación los conceptos de consulta automatizada o acceso directo a una base de datos automatizada de otra instancia de tal forma que pueda obtenerse respuesta automática a la consulta, el marcado y el bloqueo de datos personales para limitar su tratamiento.

De la misma manera, es interesante notar que estas disposiciones generales sólo serán de aplicación a los datos que se transmitan o se hayan transmitido en virtud de las previsiones del Convenio y no al resto de datos personales tratados en el ámbito nacional o transmitidos por las distintas autoridades competentes en el marco de otros convenios internacionales bilaterales o multilaterales, contribuyendo, una vez más, a una regu-

lación fragmentaria y compleja de la protección de datos en el campo de la cooperación policial.

También constituye un elemento estándar de las regulaciones europeas en la materia la exigencia de que cualquier Parte del Convenio, para poder participar en el intercambio de datos personales, debe tener implantado en su derecho nacional un nivel de protección de datos que sea, al menos, equivalente a las previsiones del Convenio 108 y la Recomendación (87) 15 del Consejo de Europa.

Sin embargo, el Convenio de Prüm introduce una novedad importante: la inclusión de las previsiones del «Protocolo Adicional al Convenio para la protección de las personas en relación con el tratamiento automatizado de datos personales en relación con autoridades de control y transferencias internacionales»[17], de 8 de noviembre de 2001 como un componente más del contenido mínimo de las normas de protección de datos de cada Estado Parte del Convenio.

Ello lleva consigo la obligatoriedad de la existencia de una autoridad de control «independiente» que supervise los tratamientos de datos encaminados a la transmisión o recepción de datos personales en el marco del Convenio de Prüm y aunque parece evidente que todos los Estados de la Unión Europea poseen esta autoridad de control independiente -por la existencia de otros tratados y convenios que así lo establecen- y que con toda seguridad serán también las llamadas a supervisar estos nuevos procesos, será necesario revisar la legislación nacional para comprobarlo[18].

---

[17] Como ya se ha hecho notar con anterioridad, el texto se puede consultar en http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/

[18] En concreto, en el caso español, podrían aparecer ciertos problemas. En efecto, como hemos visto, el objetivo fundamental del Convenio es incrementar la cooperación en la lucha contra la delincuencia internacional y, en concreto, contra el terrorismo. Además, uno de sus apartados específicos, en el que se prescribe el intercambio de datos, lleva el epígrafe específico de Medidas para la prevención de atentados terroristas.

Pues bien, en virtud de la *Disposición Transitoria Primera de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)*, la Agencia Española de Protección de Datos es el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Por lo tanto, la autoridad encargada de la supervisión de estos tratamientos, salvo decisión específica en contrario del legislador, es la Agencia Española de Protección de Datos, cuya competencia se limita a los tratamientos de datos personales incluidos en el ámbito de aplicación de la LOPD o a los que la misma se les aplica con carácter supletorio.

En relación con el principio de finalidad, el artículo 35 proporciona una regla clara, también presente en otros convenios similares: la Parte que recibe la información, ya sea tras una consulta o comparación de los índices de referencia de perfiles de ADN o dactiloscópicos, ya sea mediante el acceso directo a los registros de matriculación de vehículos o por cualquier otro cauce de los previstos en el Convenio, sólo podrá utilizar los datos personales obtenidos para la finalidad para la que fueron transmitidos.

Si la Parte receptora desea utilizar dicha información con otro propósito o finalidad, deberá solicitar la autorización de la Parte que remitió la información, que sólo podrá darla si es lícita de acuerdo con su derecho nacional. Además, la parte receptora tratará los datos con la nueva finalidad al amparo de lo establecido en su derecho interno.

Lo que no aclara la disposición es si esa finalidad para la que autoriza el uso la Parte titular de los datos que se desean utilizar debe de ser una de las contempladas por el Convenio o por el contrario, el acuerdo de dicha Parte es suficiente para la utilización con cualquier otra finalidad, siempre y cuando la misma sea compatible con las normas nacionales de ambos Estados. Aparentemente, del tenor literal de la misma se desprende que si la nueva finalidad autorizada está contemplada por las normas nacionales, podría ser completamente distinta de las que motivan la adopción del Convenio, lo que no parece que debiera ser la opción más adecuada. Por ello, el eventual Acuerdo de Ejecución que suscriban las Partes debería aclarar este punto.

No obstante, lo que sí se echa en falta es la necesidad de que la Parte que pretende la utilización de los datos con una finalidad diferente no tenga la obligación de motivar las razones que le llevan a solicitar la autorización

---

Pero en la letra c) del apartado segundo del artículo segundo de la Ley Orgánica 15/1999 se excluyen explícitamente del ámbito de aplicación de la misma *"… a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada"* y, por ello, como los ficheros de los cuales es obvio que saldrá la información para la cooperación antiterrorista y el intercambio de información en el marco del Convenio de Prüm serán, precisamente, aquéllos constituidos para luchar contra el terrorismo y la delincuencia organizada, la situación dista mucho de ser clara y pacífica desde el punto de vista jurídico.

Aunque, a fuer de sinceros, las Partes firmantes del Convenio parecen haber dado carpetazo a este asunto mediante el apartado segundo de la Declaración Conjunta adjunta al Convenio ya que en el mismo se establece *"…que, por lo que respecta a la segunda frase del apartado 2 del artículo 34, a) en el momento de la firma se cumplen ya, en lo sustancial, las condiciones para la transmisión de datos de carácter personal en virtud del capítulo 7 del Tratado, en la medida en que no se refieren a la consulta o la comparación automatizadas de datos, b) crearán lo antes posible las condiciones previstas en el Capítulo 7 que todavía no se cumplen, en particular en materia de consulta o comparación automatizadas"*.

para ello y que dicha justificación, junto con la respuesta positiva o negativa de la Parte titular de los datos, queden registradas para su posterior verificación a efectos del posible establecimiento de responsabilidades si se produce un tratamiento o requerimiento irregular o malicioso. Ello tiene su importancia incluso desde el punto de vista de la responsabilidad por daños y perjuicios en que se pudiera incurrir.

Por otro lado, los datos transmitidos al amparo de los artículos 3, 4 y 9, esto es, los obtenidos por consulta o comparación en los índices de referencia de perfiles de ADN y dactiloscópicos, tienen un régimen más estricto, ya que sólo pueden ser utilizados para comprobar si existen o no coincidencias con los datos comparados, para la preparación y presentación de una solicitud de asistencia administrativa o judicial o para su registro a efectos de constancia de la consulta para la verificación de la licitud de la misma según establece el artículo 39.

Además, la Parte que recibe la consulta sólo podrá tratar los datos que se le han transmitido con ese propósito para llevar a cabo la comparación, la respuesta automatizada o el registro de auditoría y éstos se cancelarán inmediatamente tras responder a la consulta, salvo que sean necesarios para su registro con fines de comprobación de la legalidad o para la preparación de solicitud de asistencia.

Por su parte, los datos recibidos como resultado de una consulta directa al registro de vehículos de otra Parte contratante sólo podrán utilizarse por la Parte requirente en el procedimiento que dio lugar a la consulta. La Parte titular del registro de vehículos que proporciona la respuesta deberá obrar de manera similar a la descrita en el párrafo anterior.

Los datos de carácter personal transferidos al amparo del Convenio sólo podrán ser utilizados por las autoridades y tribunales competentes para desempeñar una función en el marco de los fines que se prevén en el artículo 35 que acabamos de analizar. Ello significa que si, como hemos concluido, del estudio pormenorizado del mismo se deduce que existe una cierta vaguedad en las finalidades para las que los datos pueden ser utilizados, esta misma vaguedad se trasladará a la determinación de las autoridades competentes. Además, el artículo 33 «in fine», permite la transferencia ulterior a otras «instancias»[19] –ni siquiera habla de otras autoridades, lo que abre la puerta a una nueva indefinición de los posibles destinatarios finales de los datos- si la Parte titular de la información así lo autoriza, sin

[19] El Diccionario de la Real Academia Española define “Instancia” como “Institución, organismo” o “Nivel o grado de las Administraciones Públicas”, lo que le otorga un significado extraordinariamente amplio.

que exista ningún otro requerimiento vinculado a la finalidad de la transferencia ulterior. Para evitarla, debería definirse claramente qué significa exactamente el término otras instancias, bien sea mediante la enunciación de dichas instancias: servicios de policía, jueces y magistrados, etc. o bien mediante una lista de autoridades a las que pudieran remitirse los datos en cada una de las Partes y de los servicios autorizados a recibir la información, todo ello de acuerdo con el derecho nacional aplicable.

Seguidamente, en el artículo 37, se estable el régimen sobre exactitud de los datos personales, su actualización y periodos de retención de la misma. Como norma general, se establece la obligación de las Partes de velar por que la información sea exacta y se encuentre actualizada en todo momento además de la obligación de rectificar o cancelar de oficio o a petición del titular de los datos aquéllos que fueran inexactos o se hubieren transmitido indebidamente.

Si una persona alega que determinados datos no son exactos pero dicha afirmación no puede confirmarse o negarse, los datos se marcarán a petición del interesado para señalar su disconformidad, si el derecho nacional de la Parte lo permite. Dicha marca sólo podrá borrarse con el consentimiento del interesado o mediante resolución judicial o de la autoridad de protección de datos.

Respecto del régimen de cancelación, la primera regla es que los datos personales se cancelarán siempre que los mismos no hubieran debido transmitirse. Por otro lado, los datos que se hayan transferido de forma lícita se cancelarán siguiendo las reglas comúnmente aceptadas en Europa por las normas de protección de datos, es decir, cuando no sean necesarios o hayan dejado de serlo para el fin para el que se transmitieron. Si los datos se transmitieron de oficio sin mediar requerimiento de la Parte receptora, ésta debe comprobar sin dilación si se necesitan para el fin que haya justificado su transmisión.

Por lo demás, para los periodos máximos de retención de los datos personales, el Convenio se remite a los plazos marcados en el derecho interno de la Parte que envió la información, siempre y cuando la misma hubiera informado de los mismos en el momento de remitirla. De esta manera los plazos de retención de los datos personales pueden ser –y de hecho son- completamente diferentes en función del Estado que remita la información. Si a ello le añadimos que el efectivo cumplimiento de los mismos depende de la discrecionalidad en su comunicación por parte de quien remite la información y la complejidad de gestionar una importante variedad de estos plazos de cancelación, vemos que esta regulación tiene

un amplio margen de mejora y homogeneización que quizás lleve a cabo la Decisión Marco que hemos mencionado al comienzo de este documento.

Finalmente, se establece que una vez pasados los plazos máximos de conservación, los datos personales deberán ser suprimidos, salvo que existan motivos para creer que la supresión podría afectar a intereses dignos de protección de la persona concernida, en cuyo caso, siempre de acuerdo con el derecho nacional, los datos serán bloqueados y solo podrán transmitirse o utilizarse para el fin por el que se prescindió de su supresión.

Por lo que respecta a la adopción de las necesarias medidas de seguridad, el Convenio se limita a una formulación genérica respecto de que todas las Partes adopten las medidas necesarias para garantizar la disponibilidad (protección frente a destrucción o pérdida, ya sean fortuitas, accidentales o intencionadas), confidencialidad (protección frente al acceso y divulgación no autorizado) e integridad (protección frente a su modificación fortuita o no autorizada), remitiéndose al Acuerdo de Ejecución para mayores precisiones.

No obstante, en relación con el contenido mínimo que obligatoriamente constará en el futuro Acuerdo de Ejecución, el apartado segundo del artículo 38 dispone que, en el ámbito de las consultas automatizadas, dicho Acuerdo deberá contemplar las medidas acordes con el estado de la técnica en cada momento para garantizar la integridad y confidencialidad de los datos. Asimismo, señala que cuando se utilicen redes de acceso general (debiéndose entender en la terminología habitual, redes públicas de comunicaciones), se apliquen los procedimientos de codificación y autenticación homologados por los órganos competentes para ello (es de suponer que cuando se habla de codificación se está haciendo referencia a técnicas de enmascaramiento de la información como, por ejemplo, la criptografía o la esteganografía, excluyendo otros métodos menos fiables como la mera compresión de la información) y, finalmente, la descripción de los mecanismos de registro y auditoría de las transacciones para garantizar su legalidad y admisibilidad, que se tratan en el siguiente artículo.

En efecto, el artículo 39 se dedica a la constancia documental de los intercambios de información realizados en virtud del Convenio para posibilitar la posterior verificación del cumplimiento de los requerimientos presentes en el mismo. Para ello, el artículo 39 divide la consideración del régimen de este registro en dos partes: la correspondiente a las transmisiones y recepciones no automatizadas y a las que se realizan por aplicación de lo previsto en los artículos 3, 4, 9 y 12 (los referidos a consulta automatizada de perfiles de ADN, datos dactiloscópicos y registros de vehículos así como a la comparación automatizada de perfiles abiertos de ADN).

Con ello, aparece una primera cuestión que habrá de dilucidarse y es aquélla referida al posible «limbo jurídico» al que puede quedar relegado el control de legalidad de aquellas transferencias de datos personales que se realicen por medios automatizados pero no estén comprendidas en las previstas en los artículos 3, 4, 9 y 12. En efecto, el artículo 39 establece un régimen de registro de los intercambios para las transferencias no automatizadas –esto es, las que se realizarían sin la utilización de las modernas tecnologías de la información y las comunicaciones, por procedimientos tradicionales basados en el papel- y otro específicamente diseñado para los accesos a los índices de referencia de perfiles de ADN y dactiloscópicos así como a los datos de matriculación.

Pero si repasamos los distintos tipos de intercambio de datos previstos en el Convenio, nos daremos cuenta que nada impide que se intercambien de forma automatizada datos, por ejemplo, sobre sospechosos de terrorismo o de cometer delitos en grandes eventos transfronterizos y, dado que dichas transferencias no están previstas en los artículos reseñados, la lectura literal del Convenio lleva a la conclusión de que no se exige el registro de las mismas.

Dado que el legislador ha optado por establecer un régimen exigente a la hora de registrar todos los intercambios de los datos mencionados, sería razonable entender que cuando el Convenio habla de transferencia no automatizada, en este artículo, está en realidad estableciendo el régimen general de registro y, posteriormente, instaurando un régimen especial para los accesos automatizados a ciertos tipos de datos que requieren especiales salvaguardias. Esta interpretación que es sin duda la más coherente con el espíritu que parece animar al legislador no es en absoluto evidente y, por ello, una vez más, sería deseable que el futuro Acuerdo de Ejecución clarificara el régimen de registro para ese tipo de transferencias.

En este entendimiento, cualquier intercambio de datos personales amparado por el Convenio debe de registrarse de forma que quede constancia documental del mismo en los términos previstos en el apartado primero del artículo 39, de suerte que cada una de las Partes implicadas en una transmisión garantizará la documentación, registrando el motivo de la transmisión, los datos transmitidos, la fecha de la transmisión y la designación o identificación de la instancia que realiza la consulta y de la titular del fichero.

Por su parte, el apartado segundo, establece las reglas por las que debe regirse la consulta automatizada de datos en virtud de los artículos 3, 9 y 12 y la comparación automatizada en virtud del artículo 4. Los aspectos fundamentales de dicha regulación se resumen a continuación.

En primer lugar, sólo los agentes especialmente autorizados de los puntos nacionales de contacto podrán llevar a cabo estas operaciones, debiendo existir una lista de los mismos que se pondrá a disposición del resto de las Partes así como de la autoridad de supervisión de protección de datos.

Además, cada Parte Contratante garantizará que quede registrada toda transmisión y toda recepción de datos por la autoridad titular del fichero y por la autoridad que realice la consulta, incluida la comunicación de la existencia o inexistencia de concordancias. Los elementos que contendrá dicho registro serán los datos transmitidos, la fecha y hora exacta de la transmisión y la designación o identificación de la autoridad que realice la consulta y la titular del fichero. Igualmente, la autoridad que realice la consulta registrará asimismo el motivo de la misma o de la transmisión y la identificación del agente que la realizó, así como del agente que originó la consulta o transmisión.

Los datos de estos registros quedarán a disposición de las autoridades de supervisión en materia de protección de datos de las partes implicadas en cada una de las transmisiones, que podrán requerir su comunicación en cualquier momento. Dicha solicitud deberá ser contestada en un plazo máximo de cuatro semanas, aunque el Convenio establece que la solicitud debería ser respondida «inmediatamente»[20].

Los datos contenidos en los registros sólo podrán utilizarse para el control del cumplimiento de las normas sobre protección de los datos y la garantía de la seguridad de los mismos, deberán protegerse contra su utilización indebida y se cancelarán al cabo de dos años.

El último apartado del artículo 39 instaura el régimen de control jurídico de las transmisiones de datos de carácter personal. En primer término, dispone que el órgano independiente competente para dicho control jurídico sea la autoridad de protección de datos designada por cada una de las Partes. Con arreglo al derecho interno, cualquier persona podrá solicitar a dicha autoridad que examine la legalidad del tratamiento de datos sobre su persona[21].

---

[20] Llama la atención la expresión utilizada para describir el derecho de las autoridades de control en materia de protección de datos a conocer el contenido de dichos registros. El Convenio utiliza el término *comunicará* lo que podría excluir la posibilidad de que sean las propias autoridades de control las que verifiquen por sí mismas el contenido de dichos registros.

[21] Esta previsión legal puede resultar de difícil interpretación en el Derecho español, ya que es una disposición típica de aquellos Estados que se han dotado de un régimen de *acceso indirecto* a los datos personales tratados por las fuerzas y cuerpos de seguridad. En

A dichas autoridades de protección de datos, al igual que a los órganos competentes en la gestión de los registros documentales -instancias competentes del registro- se les impone la obligación de realizar controles por muestreo de la legalidad de las transmisiones sobre la base de los expedientes relativos a dichas consultas, debiendo conservarse los resultados derivados de esta actividad de control durante un periodo de dieciocho meses, cancelándose inmediatamente una vez transcurrido dicho plazo.

Igualmente, las autoridades de control de protección de datos deberán cooperar entre sí para el desempeño de sus funciones y, en particular, mediante el intercambio de las informaciones necesarias y el ejercicio de sus poderes en el territorio de una Parte a petición de la autoridad de control de otra de las Partes Contratantes. Todo ello deberá llevarse a cabo de acuerdo con el derecho interno de cada una de las partes.

Finalmente, el último aspecto que abordan las disposiciones generales sobre protección de datos –salvo una mención a la obligación de informar a la Parte transmitente, a requerimiento de ésta, sobre el destino y los objetivos conseguidos con el tratamiento de los datos transmitidos– es el de los derechos de los afectados y la posible indemnización por daños y perjuicios.

---

este tipo de regímenes jurídicos, el interesado no ejerce su derecho de acceso directamente ante la autoridad policial de que se trate, sino que debe dirigirse a la autoridad de control en materia de protección de datos para que sea ella la que acceda en su nombre y verifique la legalidad de los tratamientos. Además, normalmente, en este tipo de sistemas, el ciudadano nunca recibe una respuesta concreta a su petición, sino, en la mayor parte de los casos, una respuesta neutra de la que no pueda traslucirse información que pudiera ser utilizada por grupos criminales, a través de varias solicitudes de mala fe, para obtener información indirecta de la situación sobre los datos personales de sus miembros que obran en poder de las fuerzas policiales.

En el caso de la legislación española, al haber optado el legislador por un acceso directo a sus datos personales por parte de los ciudadanos, la Agencia Española de Protección de Datos y las agencias autonómicas, poseen una clarísima competencia para tutelar el derecho de aquellos ciudadanos a los que los cuerpos de seguridad se lo hayan denegado, pero no tiene una competencia claramente atribuida para ejercer esta función de verificación, aunque siempre podría realizar una investigación a tenor de una denuncia presentada por un ciudadano, pero no es ese el espíritu de la verificación de la legalidad a la que se refiere el Convenio.

No obstante, parece ser que en el estado actual de los trabajos es posible que este *"derecho de verificación"* se contemple en el nuevo Reglamento de desarrollo de la LOPD en el que está trabajando el Ministerio de Justicia y que, de esta manera, se dote a la Agencia Española de Protección de Datos de la competencia de verificar la licitud de los tratamientos de datos personales vinculados a los ficheros creados para la lucha contra el terrorismo y las formas graves de delincuencia organizada en unos términos similares a los que existen en las legislaciones de otros países antes mencionadas, es decir, informando al interesado de que se ha llevado a cabo la verificación pero sin ofrecer ninguna información adicional.

En primer lugar, el artículo 40 afirma el derecho de acceso de los afectados a «…los datos relativos a su persona que hayan sido objeto de tratamiento, así como de su procedencia, destinatario o categoría de destinatario, fin previsto para el tratamiento y fundamento jurídico del mismo». Este acceso deberá llevarse a cabo tras la oportuna acreditación de la identidad y conforme al derecho interno. Además, se establece que la información deberá facilitarse «… sin unos costes desproporcionados, de forma generalmente comprensible y sin demoras indebidas».

Esta formulación tiene dos aspectos fundamentales. El primero de ellos es muy positivo y consiste en la afirmación rotunda del derecho de acceso a los datos personales tratados en base al Convenio por cualquier afectado, sin establecer ningún tipo de restricción en su ejercicio. El segundo punto es que, tras el establecimiento de este principio general, se deja la regulación material de su contenido al derecho interno de cada una de las Partes y esto, como se demuestra en el documento «The Schengen Information System. A guide for exercising the right of access»[22], equivale a introducir un régimen fraccionado, complejo y de difícil aplicación cuando concurren los intereses o la intervención de varias Partes Contratantes.

No es este el lugar para extenderse en una explicación detallada de los distintos regímenes jurídicos para el ejercicio del derecho de acceso por parte de los ciudadanos, pero baste señalar para ilustrar el punto anterior que dependiendo del Estado Parte del Convenio de Schengen en el que una persona decida solicitar su derecho de acceso, el procedimiento y las formalidades requeridas para hacerlo, la autoridad a la que debe dirigirse, la información que obtendrá, la respuesta que se le proporcione y los mecanismos de recurso contra la decisión, caso de no resultar satisfactoria, serán completamente distintos.

Por el contrario, la regulación de los derechos de rectificación y cancelación es bastante más nítida «… la persona concernida tendrá derecho a que se rectifiquen los datos inexactos y se cancelen los datos tratados de forma ilícita». No obstante, basándonos en la regla general que aparece en el tercer inciso del apartado primero del artículo 40, esto es, que «… los pormenores del procedimiento para el aseguramiento de estos derechos y las razones de limitación del derecho a la información se regirán por el derecho interno del Estado en el que se hagan valer esos derechos», debemos entender que, al igual que en el derecho de acceso, las limitaciones

[22] Documento elaborado por la Autoridad Común de Control de Schengen. Se puede acceder a su contenido en http://www.schengen-jsa.dataprotection.org/ dentro del canal "Safeguards for citizens".

y excepciones a estos derechos se dejan en manos del derecho nacional de la Parte ante la que se invoca el derecho y se solicita la rectificación o cancelación.

El Convenio también obliga a que las Partes Contratantes garanticen que aquellos afectados que hayan visto lesionados su derecho fundamental a la protección de datos personales puedan presentar una reclamación ante un tribunal independiente e imparcial en el sentido de lo prevenido por el apartado primero del artículo 6 del Convenio Europeo de Derechos Humanos y Libertades Fundamentales, así como ante una autoridad de control independiente en el sentido del artículo 28 de la Directiva 95/46/CE, y que tenga la posibilidad de que los tribunales le reconozcan el derecho a la indemnización de daños o a una compensación de otro tipo.

En el segundo apartado de este mismo artículo, se describe el régimen de responsabilidades de las distintas Partes por la utilización de datos transmitidos no exactos. En concreto, el apartado segundo del artículo 40 afirma que «…cuando un órgano de una Parte Contratante transmita datos de carácter personal en virtud del presente Tratado, la instancia receptora de la otra Parte Contratante no podrá, en relación con su responsabilidad con arreglo al derecho interno, alegar en su descargo frente al perjudicado que los datos transmitidos no eran exactos».

Pero, a continuación, prevé los mecanismos de compensación para que una Parte se resarza del importe abonado a una persona en concepto de daños y perjuicios ocasionados por una información inexacta o errónea remitida por otra Parte Contratante cuando afirma que «… si la instancia receptora indemniza los daños causados por la utilización de datos transmitidos inexactos, el órgano transmitente deberá rembolsar a la instancia receptora el importe total de la indemnización de daños abonada».

7. CONCLUSIONES

En primer lugar y como acertadamente ha señalado el Supervisor Europeo de Protección de Datos en su «Dictamen sobre la propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad»[23], la conclusión del Convenio de Prüm al margen de las instituciones de la Unión supone una falta de control democrático por parte del Parlamento Europeo –aunque es bien cierto que de-

[23] Diario Oficial de la Unión Europea Nº C 116, de 17 de mayo de 2006, pp. 8 a 17. El texto se encuentra disponible en la dirección web siguiente: http://eur-lex.europa.eu/LexUriServ/site/es/oj/2006/c_116/c_11620060517es00080017.pdf

berá ser aprobado por los Parlamentos nacionales de las Partes– y de control judicial por parte del Tribunal de Justicia de las Comunidades Europeas. O dicho de otra manera, las instituciones de la Unión Europea no han tenido ni tendrán la posibilidad de valorar con carácter previo al establecimiento de los mecanismos de cooperación previstos en el Convenio el impacto de sus previsiones en el derecho fundamental a la protección de datos de carácter personal.

No obstante, por otra parte, el enfoque del Convenio de Prüm –conocido como «campo de datos por campo de datos»– definiendo un conjunto específico de tipos de datos para su intercambio en los términos recogidos en el Convenio y no regular una transferencia general e indeterminada de cualesquiera tipologías de datos, es positivo en dos aspectos. El primero de ellos tiene que ver con una aplicación más cautelosa del principio de proporcionalidad, ya que al restringir las categorías de datos que pueden transferirse permite obtener un conjunto de experiencias prácticas que ayudarán a decidir sobre la necesidad o no de una ampliación de estos intercambios, suponiendo, además, una menor intrusión en la privacidad de las personas.

En segundo lugar, la opción, al menos en los casos más sensibles, a favor de la utilización de índices de referencia en lugar de por un acceso directo a las bases de datos nacionales, también establece un primer filtro para el acceso a la información directamente personalizada. Sólo se produce un acceso efectivo a datos directamente atribuibles a personas físicas y a la identificación efectiva de aquellas a las que se pueden referir las consultas y comparaciones tras verificarse que existe una coincidencia en las bases de datos de índices de referencia.

Sin embargo, también hay que señalar que, desde el punto de vista de la proporcionalidad, existe una clara carencia en el articulado del Convenio respecto de la definición de los datos personales que se podrán intercambiar por aplicación de los artículos 5, 10 y 14 que impide evaluar adecuadamente si los mismos han de considerarse adecuados, pertinentes y no excesivos en relación con la finalidad para la que son intercambiados.

Por ello, sería necesario que estos aspectos se aclararan en el posterior Acuerdo de Ejecución[24], durante cuya gestación debería darse la opor-

[24] En el momento de finalizar este trabajo y a través de informaciones aparecidas en diversos medios de comunicación se ha tenido noticia de la firma, el día 5 de diciembre, en Bruselas, del Acuerdo de Ejecución del Tratado de Prüm. No obstante, al cierre de este artículo, el autor no dispone del texto definitivo de dicho Acuerdo de Ejecución y, por ello, no le es posible comentar su contenido en lo que afecta a las consideraciones hechas sobre el

tunidad de intervenir y dar su opinión a las autoridades de protección de datos de los Estados firmantes del Convenio y de aquellos de los que se prevea una pronta adhesión al mismo.

Otra característica que es importante destacar es la «nacionalización» de las previsiones jurídicas del Convenio. En efecto, las referencias a la aplicabilidad del derecho interno de las Partes son continuas y consistentes a lo largo de todo el articulado. Este hecho, que viene motivado por la estructura nacional de las bases de datos que se crean o utilizan para intercambiar datos –lo cual, tiene el aspecto positivo de no generar una gran acumulación de datos personales en una base de datos centralizada, lo que sería una medida más intrusiva para la privacidad de las personas– genera que convivan una multitud de regímenes jurídicos distintos y diversos que, en el apartado específico de la protección de datos, no ayuda a un conocimiento cabal y predecible por todas las Partes de las normas que regulan los intercambios de información y lo torna aún más difícil para aquellos afectados que deseen saber cuales son las aplicables en cada caso y la forma y manera en que han de ejercer sus derechos.

Estas disposiciones de derecho interno son las que regularían, entre otras cuestiones, aspectos tan cruciales para la protección de datos personales como las reglas sobre el tratamiento y cesión de datos sensibles, completamente ausentes del Convenio, el deber de secreto y la confidencialidad que todos los que participan en los tratamientos deben mantener y las obligaciones sobre la notificación y, en su caso, el control previo de los tratamientos por parte de las autoridades nacionales de protección de datos.

Por todo ello, la puesta en marcha de las previsiones del Convenio de Prüm que, como se trató al principio de este trabajo, han de considerarse como un aspecto más de las medidas encaminadas a poner en marcha el llamado Principio de Disponibilidad, debería de llevarse a cabo sólo tras la implantación de los requisitos establecidos en el Programa de La Haya y, en particular, tras la necesaria armonización de las normas de protección de datos de los Estados miembros de la Unión Europea, como una medida compensatoria absolutamente necesaria ante el incremento exponencial de

---

mismo a lo largo de este documento. Si se desea, se pueden consultar los comentarios que sobre un borrador fechado en el mes de julio de 2006 realizaron las autoridades de protección de datos de los Estados signatarios del Tratado reunidas informalmente en Bonn (República Federal Alemana), el 27 de julio de 2006 en http://www.statewatch.org/news/2006/sep/dpa-opinion-prum-06.pdf. Sobre el mismo borrador, se puede examinar la reacción de la CNIL (autoridad de protección de datos francesa) en http://www.statewatch.org/news/2006/sep/cnil-fr-opinion-prum-06.pdf.

los datos personales que serán intercambiados en el marco de la cooperación policial.

Así pues, la adopción de la «Decisión Marco sobre Protección de Datos en el ámbito de la cooperación policial en materia de derecho penal», con un contenido próximo a la propuesta de la Comisión Europea y aplicable a todo el proceso de tratamiento de datos personales en el ámbito policial en los Estados miembros, es una cuestión que se torna cada vez más urgente para dotar de seguridad jurídica a todos los proyectos de incremento y mejora de la cooperación policial que se están poniendo en marcha en Europa.

RESUMEN

La firma y ratificación del Convenio de Prüm significa la puesta en marcha del concepto acuñado por el Programa de La Haya como «Principio de Disponibilidad» de una manera limitada y sectorial, definiendo un conjunto limitado de tipologías de datos como perfiles de ADN, huellas dactilares, datos sobre vehículos o sobre sospechosos de terrorismo y estableciendo reglas «ad hoc» para su intercambio y tratamiento.

Todo ello se lleva a cabo con unos objetivos tan genéricos como el luchar con mayor eficacia contra el terrorismo, la delincuencia transfronteriza y la migración ilegal. Además, todas sus disposiciones y, en particular, las relativas a la protección de datos personales, se basan en las legislaciones nacionales de las Partes, lo que introduce un régimen fragmentario y un mosaico de normas jurídicas aplicables que no contribuyen a la transparencia y el conocimiento y ejercicio de sus derechos por parte de los ciudadanos.

PALABRAS CLAVE: Tratado de Prüm, Principio de Disponibilidad; ADN; Huellas Dactilares; Terrorismo, Migración Ilegal, Protección de Datos, Datos Personales

ABSTRACT

The signature and ratification of the Treaty of Prüm is the first practical implementation of the concept coined by The Hague Programme as «Principle of Availability». This is done in a limited manner and in specific sectors, defining the exchange of a limited set of data types like DNA profiles, fingerprints, data about vehicles or suspects of terrorist activities and setting up «ad hoc» rules for their exchange and processing.

All these actions are carried out with very general objectives like a more efficient fight against terrorism, the international forms of crime and illegal immigration. Besides,

all its provisions and, in particular, those related with data protection, are based in the national law of the Contracting Parties, what introduces a fragmentary regime and a mosaic of applicable legal rules that do not contribute to the transparency on its application and to the harmonised exercise of their rights by the citizens.

KEYWORDS: Treaty of Prüm, Principle of Availability, DNA, Fingerprints, Terrorism, Illegal Migration, Data Protection, Personal Data.