

ES

ES

ES



COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas, 24.11.2005
COM(2005) 597 final

**COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO
EUROPEO**

**sobre una mayor eficacia, interoperabilidad y sinergia entre las bases de datos europeas
en el ámbito de la Justicia y los Asuntos de Interior**

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO

sobre una mayor eficacia, interoperabilidad y sinergia entre las bases de datos europeas en el ámbito de la Justicia y los Asuntos de Interior

1. CONTEXTO

En varias ocasiones, y en el contexto de la lucha contra el terrorismo y la mejora de la seguridad interna, tanto el Consejo Europeo como el Consejo de la Unión Europea han pedido a la Comisión que presente propuestas sobre una mayor eficacia, interoperabilidad y sinergia entre las bases de datos europeas (Declaración de 25 de marzo de 2004 sobre la lucha contra el terrorismo¹, Programa de La Haya² y Declaración del Consejo de 13 de julio de 2005 tras los bombardeos de Londres).

El Consejo Europeo y el Consejo también han subrayado repetidamente la importancia de utilizar datos biométricos en bases de datos y documentos de viaje para aumentar el nivel de seguridad en la Unión Europea.

2. DEFINICIONES Y OBJETO DE LA PRESENTE COMUNICACIÓN

2.1. Objeto de la presente Comunicación

El contexto en el que se realizó la petición de elaborar la presente Comunicación – la lucha contra el terrorismo y la delincuencia - indica que su propósito va más allá de una mejora sustancial de la interoperabilidad técnica y de la sinergia entre los sistemas de tecnología de la información (TI) en el ámbito de la Justicia y los Asuntos de Interior.

La finalidad de esta Comunicación es explicar de qué manera, más allá de sus objetivos actuales, podrían estos sistemas apoyar más eficazmente las políticas relacionadas con la libre circulación de personas y contribuir al objetivo de luchar contra el terrorismo y la delincuencia grave.

Es necesario encontrar un equilibrio sutil entre la consecución de estos objetivos y la protección de los derechos fundamentales (especialmente la protección de los datos personales), según lo dispuesto en el Convenio Europeo de Derechos Humanos y en la Carta de los Derechos Fundamentales de la Unión Europea. También hay que tener en cuenta que los sistemas de TI pueden servir para proteger y desarrollar los derechos fundamentales del individuo.

¹ Consejo de la Unión Europea 7906/04 Declaración sobre la lucha contra el terrorismo, 29 de marzo de 2004.

² Programa de la Haya sobre refuerzo de la libertad, la seguridad y la justicia en la Unión Europea, 10 de mayo de 2005.

La presente Comunicación pretende suscitar un debate profundo sobre la forma y la arquitectura a largo plazo de los sistemas de TI. Al identificar las distintas situaciones posibles, incluidas las de gran envergadura en cuanto a su ambición e impacto, esta Comunicación no prejuzga los resultados de un debate profundo ni juzga cuándo ni en qué condiciones deberán crearse esas situaciones, si es que se crean. Asimismo, dado su enfoque político y estratégico, no aborda ni evalúa detalladamente el impacto jurídico³, técnico, organizativo o social de las posibles soluciones. Antes de realizar cualquier acción legislativa, deberán realizarse análisis de impacto detallados, especialmente desde el punto de vista de la proporcionalidad. Estos análisis también deberán estudiar el impacto que las soluciones previstas podrían tener en otros medios de cooperación, actuales o en proyecto, entre las autoridades responsables de la seguridad interna (por ejemplo, en el marco de Europol).

La presente Comunicación comienza con una breve descripción de la situación actual de los sistemas de TI paneuropeos existentes y futuros, así como de las deficiencias observadas en la consecución de sus objetivos actuales. En un segundo momento, se presentan las situaciones previstas para una utilización más eficaz de estos sistemas y para la creación de futuros sistemas. Por último, se examina si las posibilidades técnicas y operativas son proporcionadas y compatibles con la necesidad de proteger los derechos de la persona.

La presente Comunicación no propone medidas destinadas a reforzar la interoperatividad ni a crear sinergias a escala nacional. Aunque las medidas que se adopten a nivel europeo pueden producir efectos en los sistemas nacionales, corresponde a cada Estado miembro analizar los medios para que los sistemas nacionales interactúen mejor.

2.2. Conceptos

Antes de entrar en el detalle del análisis, deben aclararse los conceptos siguientes.

Por "*interoperatividad*" se entiende la "capacidad para compartir e intercambiar información y conocimientos de los sistemas de tecnologías de la información y las comunicaciones (TIC) y de los procesos empresariales en que se basan"⁴. La "*interoperatividad*" es un concepto técnico más que jurídico o político. No está vinculado a la cuestión de si el intercambio de datos es legal o políticamente posible o necesario⁵.

La "*conectividad*" es un término genérico que designa la conexión de dispositivos para la transferencia de datos.

³ Incluido el alcance de la participación de los países que no participan (plenamente) en el "acervo de Schengen".

⁴ *European Interoperability Framework for Pan-European eGovernment Services*, Oficina de Publicaciones Oficiales de las Comunidades Europeas, 2004, apartado 1.1.2.

⁵ Las modalidades detalladas de la interacción técnica de las organizaciones respecto del intercambio de datos se fijan generalmente en un marco de interoperatividad, que puede definirse como un conjunto de normas y directrices, véase *European Interoperability Framework for Pan-European eGovernment Services*, Oficina de Publicaciones Oficiales de las Comunidades Europeas, 2004, apartado 1.1.2.

La "*sinergia*" tiene una dimensión técnica, económica y organizativa. Técnicamente, "*sinergia*" designa una conjunción mutuamente ventajosa de varios elementos. Desde el punto de vista económico, significa un aumento del valor de los activos o una economía de escala. Desde el punto de vista organizativo, la "*sinergia*" supone la combinación de recursos hasta entonces separados o la racionalización de la organización existente con el fin de lograr una mayor eficacia.

El "*principio de disponibilidad*" supone que las autoridades responsables de la seguridad interior en un Estado miembro o los agentes de Europol que necesiten información para la realización de sus tareas deberán obtenerla de otro Estado miembro si esta información es accesible en este último.

3. ESTATUTO Y FINALIDAD DE LOS SISTEMAS INFORMÁTICOS EXISTENTES Y FUTUROS

La presente Comunicación se centra en los sistemas en los que el Consejo Europeo y el Consejo de la Unión Europea han hecho especial hincapié, es decir los sistemas SIS II, VIS y EURODAC. Cada uno de estos sistemas persigue una finalidad concreta. Los datos personales que tratan no son necesariamente los mismos, puesto que se limitan a los que están en relación con la finalidad concreta del sistema en cuestión. Las autoridades habilitadas para acceder a los datos personales tampoco son siempre las mismas.

3.1. SIS II

El Sistema de Información de Schengen de segunda generación (SIS II) facilitará el paso de las fronteras en la Unión Europea ampliada sin comprometer la seguridad. Este sistema permite a las autoridades de los Estados miembros cooperar, intercambiando información, con el fin de establecer un espacio sin controles en las fronteras interiores. La información obtenida se utilizará para el control de las personas en las fronteras exteriores o en el territorio nacional y para la expedición de visados y permisos de residencia, así como para la cooperación policial y judicial en materia penal⁶.

3.2. VIS

El Sistema de Información sobre Visados (VIS) beneficiará a los viajeros de buena fe mejorando los procedimientos de expedición de visados. Mejorará la aplicación de la política común de visados y la cooperación consular con el fin de prevenir las amenazas para la seguridad interior y el "*visa shopping*" (presentación simultánea de varias solicitudes de visado en distintos Estados miembros en busca de las condiciones más favorables); facilitar la lucha contra el fraude; contribuir a la identificación y a la repatriación de las personas en situación irregular; y facilitar la aplicación del Reglamento Dublín II⁷.

⁶ Las condiciones relativas al tratamiento de los datos personales se definirán en los instrumentos jurídicos que regulan el SIS II.

⁷ Reglamento (CE) nº 343/2003 del Consejo, de 18 de febrero de 2003, por el que se establecen 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, DO L 50 de 25.2.2003, p. 1.

El 7 de marzo de 2005, el Consejo concluyó que sería necesario que las autoridades responsables de la seguridad interior tuvieran acceso al VIS. La Comisión presentará una propuesta que permitirá a Europol y las autoridades responsables de la seguridad interior acceder al VIS para finalidades claramente definidas.

3.3. EURODAC

EURODAC tiene por objetivo ayudar a determinar el Estado miembro responsable en virtud del Reglamento Dublín II y facilitar la aplicación de este instrumento. EURODAC es una herramienta indispensable para la eficacia del sistema europeo de asilo.

4. DEFICIENCIAS OBSERVADAS

Aunque el SIS II, el VIS y EURODAC son el objeto de la presente Comunicación, también se examinan otras cuestiones relativas a la lucha contra el terrorismo y la delincuencia.

4.1. Infraexplotación de los sistemas existentes

Actualmente, las posibilidades que ofrecen todos los sistemas existentes no están plenamente explotadas. Este es el caso, por ejemplo, de algunas categorías de descripciones personales realizadas en el SIS, como las descripciones personales a efectos de vigilancia discreta o control específico que sólo se utilizan de forma limitada y heterogénea. Una utilización mayor y más coherente de estas descripciones personales reforzaría la lucha contra el terrorismo. Por último, junto a los datos tratados en los sistemas comunes, numerosos Estados miembros mantienen listas distintas que persiguen la misma finalidad, por ejemplo las descripciones personales a efectos de no admisión, lo que supone una duplicación de esfuerzos para muchos Estados miembros.

El Reglamento EURODAC también está infrautilizado. Aunque este Reglamento obliga a los Estados miembros a tomar las huellas dactilares de todas las personas mayores de 14 años que cruzan sus fronteras irregularmente y no pueden ser devueltas, la cantidad de datos de este tipo enviados a EURODAC es una parte muy escasa del flujo migratorio total.

4.2. Limitación a las investigaciones alfanuméricas

Una investigación alfanumérica sólo puede tener éxito si la información es relativamente precisa. Por lo que se refiere a las personas, la probabilidad de no obtener resultados correctos aumenta con el tamaño de la base de datos. Cuantos más nombres contenga la base de datos, más difícil será encontrar a una persona y más probable será que la identificación sea errónea. La información errónea (por ejemplo, un nombre o una fecha de nacimiento extraído de un documento falsificado, o transcripciones diferentes de un mismo nombre) proporciona resultados falsos. Además, una investigación alfanumérica a partir de datos que no son únicos será menos precisa cuantos más datos contenga la base de datos, de modo que se obtendrán largas listas de "resultados positivos", que posteriormente será necesario

comprobar con el trabajo de muchas personas, lo que no es siempre posible en el marco de un control fronterizo.

4.3. Ninguna ventaja para los viajeros de buena fe que se desplazan con frecuencia

Entre todas las personas que piden un visado Schengen, se considera que el 20% son viajeros regulares, es decir, que piden visados frecuentemente. Para estos viajeros, las posibilidades de acelerar el trámite de la solicitud de visado son limitadas. En caso de pérdida o robo de los documentos de viaje, los viajeros de buena fe deben realizar gestiones complejas para obtener nuevos documentos de viaje.

4.4. Dificultad de identificación de los residentes ilegales

Muchos de los residentes ilegales a los que se detiene no tienen ningún documento de identificación o bien utilizan documentos falsos o falsificados. En estos casos, el proceso de identificación es largo y costoso. Si los documentos de viaje se han destruido, las autoridades no disponen actualmente de ningún sistema para comprobar la identidad.

4.5. Deficiencias en la aplicación del Reglamento Dublín II

Este Reglamento define los criterios que deben aplicarse para determinar el Estado miembro responsable del examen de las solicitudes de asilo. Uno de los criterios básicos es saber si un Estado miembro ha expedido o prorrogado un visado al solicitante de asilo. Actualmente, los Estados miembros no disponen de medios eficaces para controlar si otro Estado miembro ha expedido un visado a un solicitante de asilo, para comprobar la identidad de la persona ni para pronunciarse sobre la validez del visado.

4.6. Imposibilidad de utilizar los datos relativos al asilo, la inmigración y los visados a efectos de la seguridad interior

Por lo que se refiere al objetivo de luchar contra el terrorismo y la delincuencia, el Consejo considera ahora como una deficiencia la falta de acceso de las autoridades responsables de la seguridad interior a los datos del VIS. Se podría hacer la misma observación con respecto a los datos de inmigración contenidos en el SIS II y a los datos EURODAC. Las autoridades policiales consideran esta falta de acceso como una grave laguna para la identificación de las personas sospechosas de haber cometido una infracción grave.

4.7. El control no abarca todas las categorías de nacionales de terceros países

Actualmente el VIS sólo se refiere a los nacionales de países terceros sujetos a la obligación de visado. El control de la identidad o de la legalidad de la entrada de otras categorías de nacionales de terceros países que cruzan a menudo las fronteras, por ejemplo, los titulares de un visado para estancia de larga duración o de un permiso de residencia, o también los nacionales de países terceros no sujetos a la obligación de visado, podría también ser más eficaz. Se trata de una deficiencia que han señalado las autoridades responsables de la seguridad interna y los servicios de inteligencia.

4.8. Vigilancia incompleta de la entrada y salida de los nacionales de terceros países

Aunque el VIS permitirá comprobar el historial de las solicitudes de visado y saber si la persona que presenta el visado en la frontera es la misma a cuyo favor se ha expedido el mismo, el sistema VIS no registra las entradas de los nacionales de países terceros titulares de un visado. Tampoco guarda rastro de la salida anticipada de los nacionales de terceros países antes de la fecha de expiración de su derecho de residencia. Es decir, ni el VIS, ni el SIS II, son capaces de identificar a los residentes ilegales en la UE.

4.9. Falta de herramientas de identificación biométrica

Una de las necesidades fundamentales para las autoridades responsables de la lucha contra la delincuencia y el terrorismo es poder identificar a las personas respecto de las cuales sólo se dispone de datos biométricos, por ejemplo, una fotografía, una huella dactilar o un código de ADN. El Sistema de identificación automatizado de huellas dactilares (AFIS) y las bases de datos de ADN permiten esta identificación. Como estas bases de datos ya existen en la mayoría de los Estados miembros, los servicios de la Comisión están trabajando actualmente en una propuesta destinada a interconectar las bases de datos nacionales sobre el ADN. La Comisión también se propone presentar el año próximo un instrumento jurídico sobre las huellas dactilares. En su concepción actual, el SIS II sólo permite la introducción de una descripción personal en el sistema si se dispone al menos de una información alfanumérica básica. El hecho de que el Tratado de Prüm, firmado por siete Estados miembros el 27 de mayo de 2005, introducirá el intercambio bilateral de huellas dactilares y datos relativos al ADN en espera de la adopción de tal instrumento a nivel europeo, no hace sino resaltar esta laguna.

4.10. No existe ningún registro de ciudadanos de la Unión a escala europea

La identificación de los ciudadanos de la Unión a partir de los documentos de viaje y los documentos de identidad mejorará próximamente con la introducción de elementos biométricos. Sin embargo, aunque la mayoría de los Estados miembros dispondrán de un fichero central de los documentos expedidos y de los identificadores biométricos que correspondan a una determinada identidad, la interrogación de este fichero central sólo permitirá saber si, en este mismo Estado miembro, ya se ha expedido anteriormente un documento a la misma persona bajo otro nombre. Además, actualmente no es posible iniciar una investigación sobre una persona que, por ejemplo, esté buscada por un delito de terrorismo, para saber si a esta persona ya se le ha expedido un documento de viaje o identidad.

Se trata de una laguna que también se ha identificado en el marco de la lucha contra la usurpación de identidad, fenómeno que preocupa cada vez más a las autoridades responsables de la seguridad interior y perjudica seriamente a la economía europea.

4.11. Identificación de las víctimas de catástrofes y cuerpos no identificados

No existe ninguna base de datos suficientemente completa que permita identificar víctimas de catástrofes y cuerpos no identificados. La posibilidad de utilizar una base de datos de Interpol a tal efecto se mencionó en el Consejo. No obstante, tal base de datos no podría cubrir todos los casos.

5. OTRAS MEDIDAS POSIBLES

5.1. Una mejor utilización de los sistemas existentes

En primer lugar, se podrían utilizar de manera más eficaz los sistemas actuales explotando mejor las posibilidades existentes: mejor control de la calidad en la introducción de los datos, mayor coherencia por lo que se refiere a la introducción de las categorías de datos y mayor facilidad de uso. El lanzamiento de una consulta más amplia y más directa con los Estados miembros y el intercambio de las mejores prácticas sería útil a este respecto. Aunque esta consulta debería realizarse principalmente en los Grupos de Trabajo y los Comités existentes, la celebración de conferencias regulares con los usuarios podría aportar una contribución útil. Gracias a estas operaciones de consulta suplementarias, sería posible determinar los ámbitos en los que es necesario introducir mejoras, y sus resultados podrían entonces tenerse en cuenta en el proceso legislativo o en la práctica diaria.

Además, los Estados miembros deberían introducir y utilizar de manera más coherente algunos datos (por ejemplo, las descripciones personales en el SIS II de las personas susceptibles de cometer infracciones penales graves y los datos EURODAC sobre las personas que cruzan ilegalmente la frontera, etc).

5.2. Refuerzo de los sistemas existentes y sistemas previstos

5.2.1. Investigaciones biométricas en el SIS II

El problema que supone la identificación de personas en bases de datos que contienen millones de entradas se ha resuelto en EURODAC y se abordará en el VIS utilizando las búsquedas biométricas, que proporcionan unos resultados de una precisión sin precedentes. Las propuestas de instrumentos jurídicos relativos al SIS II permiten el tratamiento de información biométrica (fotografías e impresiones digitales). Sin embargo, habida cuenta de la configuración actual del SIS II, los datos biométricos sólo servirán para confirmar la identificación de la persona buscada (por "personas buscadas", se entenderá las "personas inscritas como no admisibles", incluidas las personas a las que deberá negarse la entrada) a partir de una búsqueda alfanumérica.

Cuando estén disponibles, las investigaciones biométricas permitirán una identificación más precisa de las personas buscadas. Sin embargo, en el SIS II sólo se almacenará la información biométrica que pueda estar vinculada legalmente a una descripción personal en este sistema.

5.2.2. Un mayor acceso por parte de las autoridades competentes en materia de asilo e inmigración al VIS y al SIS II

Las propuestas legislativas prevén el acceso de las autoridades competentes en materia de asilo al VIS y al SIS II. El VIS y el SIS II contendrán, por una parte, los datos que puedan indicar que se cumple uno de los criterios de determinación del Estado miembro responsable, es decir la expedición de un visado o una estancia ilegal en un Estado miembro. Por otra parte, VIS y SIS II podrán contener datos que completen el examen de una solicitud de asilo: los datos sobre los visados podrán ayudar a evaluar la credibilidad de una solicitud de asilo y los datos del SIS II podrán

indicar si el solicitante de asilo constituye una amenaza para el orden público o la seguridad nacional. Una comprobación en EURODAC, SIS II y VIS permitiría a las autoridades competentes en materia de asilo comprobar los datos simultáneamente en los tres sistemas.

El acceso al VIS y a algunos datos biométricos del SIS II supondría un paso decisivo en la lucha contra la inmigración clandestina. Podría identificarse fácilmente a los inmigrantes clandestinos sin papeles. También podría comprobarse más fácilmente si una persona ha entrado legalmente o no, y establecer los documentos necesarios para las personas objeto de una medida de alejamiento.

5.2.3. *Acceso de las autoridades competentes en materia de seguridad interior*

Por lo que se refiere al VIS, la Comisión acaba de presentar un proyecto de instrumento jurídico que amplía el acceso de las autoridades competentes en materia de seguridad interior a efectos de la prevención, detección e investigación de los delitos de terrorismo.

Por lo que se refiere a los datos del SIS II relativos a la no admisión, debería preverse para las autoridades responsables de la seguridad interior una extensión del acceso a estos datos a efectos de la prevención, detección e investigación de infracciones penales. Convendría articular este acceso con las otras posibilidades existentes de tratamiento de los datos relativos a las personas que constituyen una amenaza para la seguridad. Sería necesario también abordar cuestiones específicas, como la reciprocidad con los Estados miembros que no participan plenamente en las políticas vinculadas con la libre circulación de personas.

Por lo que se refiere a EURODAC, la única información disponible para identificar a una persona puede ser la información biométrica contenida en este sistema, si la persona sospechosa de haber cometido una infracción penal o un acto terrorista se ha registrado como solicitante de asilo pero no figura en ninguna otra base de datos, o sólo está registrada con datos alfanuméricos inexactos (por ejemplo, si esta persona dio una identidad falsa o utilizó documentos falsificados). Las autoridades responsables de la seguridad interior podrían así tener acceso a EURODAC en casos concretos, cuando existan buenas razones para creer que el autor de una infracción penal grave ha solicitado asilo. Este acceso no debería ser directo, sino que sería necesario pasar por las autoridades responsables de EURODAC.

El acceso a estos sistemas podría también contribuir a la identificación de las víctimas de catástrofes y de cuerpos no identificados.

5.3. **Situaciones a largo plazo y medidas futuras**

5.3.1. *Creación de un Sistema europeo automatizado de identificación penal mediante huellas dactilares (AFIS)*

Además de la propuesta ya mencionada sobre la comparación de los perfiles de ADN, podría crearse un AFIS europeo para la identificación penal, en el que se reunirían todos los datos relativos a las huellas dactilares que actualmente sólo están disponibles en los AFIS nacionales. Este sistema podría estar centralizado o descentralizado (mediante la interconexión de los AFIS existentes). Se utilizaría con

finde de investigación policial e iría más allá de la simple investigación biométrica en el SIS II descrita anteriormente, que sólo proporciona resultados positivos o negativos.

También contribuiría a la identificación de las víctimas de catástrofes y de los cuerpos no identificados.

5.3.2. *Creación de un sistema de entradas-salidas y de un sistema para facilitar el paso de las fronteras a las personas que efectúan frecuentes desplazamientos transfronterizos*

Los objetivos principales de un sistema de entradas-salidas serían controlar a las personas que entran o salen del territorio y recoger información sobre su situación por lo que respecta a la inmigración y la residencia. A su entrada y salida del territorio de la Unión Europea, los nacionales de terceros países se registrarían mediante identificadores biométricos. Ahora bien, la extensión de tal sistema de entradas-salidas a los ciudadanos de la Unión no sería posible, ya que sería incompatible con el principio de libre circulación.

Podría plantearse la cuestión de si esta solución es viable, dado el elevado número de personas que cruzan diariamente las fronteras de la Unión Europea. Con el fin de reducir los controles, se podría instaurar un programa para los viajeros de buena fe conocidos (es decir, los trabajadores fronterizos) para facilitar y automatizar el proceso de paso de las fronteras. Un programa similar funciona entre Estados Unidos, Canadá y México, en virtud del cual se entrega a los viajeros de buena fe, previa comprobación detallada de sus antecedentes, una "tarjeta de viajero de confianza" que les permite pasar la frontera siguiendo un procedimiento casi totalmente automatizado. El registro a la salida podría hacerse mediante un procedimiento de autoregistro. El incentivo para registrarse a la salida residiría en el hecho de que si no se ha registrado ninguna salida, una entrada posterior sería rechazada o sólo se concedería tras pasar por un procedimiento específico.

El sistema de entradas-salidas haría mucho más eficientes y eficaces los controles fronterizos, pero requeriría grandes esfuerzos en términos de organización, de modo que su aplicación podría resultar arriesgada y costosa. No obstante, la situación podría reexaminarse cuando el VIS esté en funcionamiento.

En cualquier caso, deberán realizarse análisis de impacto u otros análisis similares con el fin de evaluar la proporcionalidad de esta situación y las otras situaciones propuestas.

5.3.3. *Registro(s) europeos(s) de documentos de viaje y tarjetas de identidad*

La mayoría de los Estados miembros crearán sus propias bases de datos con los documentos de viaje y las tarjetas de identidad que expidan, e introducirán también los datos biométricos que se recojan al solicitar dichos documentos. La eficacia de estas bases de datos podría mejorar sensiblemente con la creación de un registro de índices a escala europea. La otra solución consistiría en interconectar las bases de datos nacionales. Cualquiera que sea la solución que se escoja, estos registros podrían contener sólo una serie de datos muy limitada (número de documento y elementos biométricos) pero permitir comprobar la autenticidad de cada documento

de viaje o identidad expedido en un Estado miembro y determinar, a partir de la información biométrica, la identidad de toda persona a la que se haya expedido un documento de viaje o identidad.

Este enfoque podría también contribuir a la identificación de las víctimas de catástrofes y de cuerpos no identificados.

5.4. Cambios arquitectónicos y organizativos

Sin entrar en un análisis detallado de los cambios técnicos y organizativos que exigiría la realización de las situaciones posibles que acaban de mencionarse, se puede considerar que el desarrollo de una arquitectura de los sistemas de información europeos orientada hacia los servicios ayudaría a maximizar las sinergias y daría lugar a inversiones de nivel realista. Una arquitectura orientada hacia los servicios garantizaría una división flexible y rentable de las funciones sin tener que fusionar los sistemas existentes. Concretamente, se podría utilizar el futuro instrumento AFIS, de alto rendimiento, que formará parte del VIS, para prestar servicios vinculados al AFIS (es decir, utilizar la investigación biométrica para otras aplicaciones, como EURODAC o, eventualmente, un registro de los pasaportes biométricos). El almacenamiento de datos y los flujos de datos podrían permanecer estrictamente disociados.

A nivel organizativo, huelga decir que la reagrupación de las actividades de gestión diaria (es decir, no necesariamente la gestión estratégica o política) de estos sistemas en una única organización crearía también importantes sinergias. La gestión de las aplicaciones dentro de una única estructura constituye por tanto una opción que debería estudiarse como objetivo a largo plazo. Con relación a los objetivos de la propuesta de programa "Libertad"⁸, la posibilidad de confiar más tarde a la Agencia de fronteras exteriores las tareas vinculadas a la gestión de los sistemas de información a gran escala (EURODAC, SIS II y VIS) es otra solución que merece estudiarse.

6. COMPATIBILIDAD DE LAS MEDIDAS POSIBLES CON LOS DERECHOS HUMANOS Y, EN PARTICULAR, LA PROTECCIÓN DE DATOS

Por lo que se refiere al objetivo de una mejor identificación de las personas buscadas, si bien es cierto que el almacenamiento de datos personales en bases de datos penales está justificado debido al comportamiento real o sospechoso de una persona (lo que debe justificarse con pruebas), no es éste el caso de EURODAC o VIS. La solicitud de asilo o de visado no indica en modo alguno que una persona hasta ahora inocente vaya a cometer una infracción penal o un acto terrorista.

El principio de proporcionalidad exige, por tanto, que estas bases de datos sólo puedan interrogarse para prevenir e investigar infracciones penales graves o delitos terroristas, o para identificar al presunto autor de una infracción penal o de un acto terrorista siempre que el interés superior de la seguridad pública lo exija, es decir, si

⁸ Propuesta de Decisión del Parlamento Europeo y del Consejo por la que se establece el Fondo europeo para los refugiados para el período 2008-2013 como parte del Programa general de solidaridad y gestión de los flujos migratorios.

el acto cometido por el delincuente o el terrorista que deba identificarse es lo suficientemente reprobable como para justificar búsquedas en una base de datos donde se registran las personas sin antecedentes penales. El umbral que deben respetar las autoridades responsables de la seguridad interior para poder buscar en EURODAC, en los datos de inmigración del SIS II o en VIS, deben ser por tanto considerablemente más elevado que el umbral que debe respetarse para poder buscar en bases de datos penales. A fin de garantizar el respeto de los derechos consagrados en los artículos 6, 7, 8, 48 y 49 de la Carta de Derechos Fundamentales de la Unión Europea, el alcance de este acceso deberá por tanto limitarse a las infracciones terroristas, según se definen en la Decisión marco 2002/475/JAI del Consejo, y a las infracciones penales que sean competencia de Europol.

Por lo que se refiere a la comparación de los perfiles ADN, la limitación a un control de resultados positivos o negativos respecto del perfil ADN únicamente (cadena alfanumérica sin ninguna otra información personal) permite respetar plenamente el principio de proporcionalidad.

El principio de proporcionalidad reviste especial importancia en relación con la posible creación de un registro europeo de documentos de viaje y tarjetas de identidad. Cabe señalar que todas las autoridades competentes en materia de protección de datos, incluidas las que acogen favorablemente la idea de crear registros nacionales, han recomendado no crear un registro europeo, debido a los riesgos de abuso. Por tanto, sólo debería preverse la creación de tal registro si el acceso al mismo estuviese estrictamente limitado y si la búsqueda en este registro se justificara por un interés superior e imperioso de seguridad pública.

Por último, en relación con todas las medidas que se prevean, es preciso hacer hincapié en el carácter indispensable de la vigilancia global por parte de los organismos competentes en materia de protección de datos. En cualquier caso, al presentar posibles propuestas futuras, la Comisión realizará, de acuerdo con la Comunicación COM (2005)172⁹, una evaluación de impacto específica sobre el respeto de los derechos fundamentales.

⁹ Comunicación de la Comisión de 27 de abril de 2005, COM (2005)172 final - Respeto de la Carta de Derechos Fundamentales en las propuestas legislativas de la Comisión - Metodología para un control sistemático y riguroso.