Dictamen del Comité Económico y Social Europeo sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (fronteras y visados) y por el que se modifican la Decisión 2004/512/CE del Consejo, el Reglamento (CE) n.º 767/2008, la Decisión 2008/633/JAI del Consejo, el Reglamento (UE) 2016/399 y el Reglamento (UE) 2017/2226

[COM(2017) 793 final — 2017/0351 (COD)]

y sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (cooperación policial y judicial, asilo y migración)

[COM(2017) 794 final — 2017/0352 (COD)]

(2018/C 283/07)

Ponente: **Laure BATUT**

Consulta	Comisión Europea, 18.1.2018
	Parlamento Europeo, 28.2.2018
Fundamento jurídico	Artículo 304 del Tratado de Funcionamiento de la Unión Europea
Sección competente	Empleo, Asuntos Sociales y Ciudadanía
Aprobado en sección	25.4.2018
Aprobado en el pleno	23.5.2018
Pleno n.º	535
Resultado de la votación	160/3/2
(a favor/en contra/abstenciones)	

1. **Conclusiones y recomendaciones**

1.1. El CESE considera útil y positiva la propuesta de la Comisión Europea de mejorar la interoperabilidad de los sistemas de información de la UE sobre fronteras y visados, así como la cooperación policial y judicial, asilo y migración.

1.2. El CESE estima que esta interoperabilidad debe ser un objetivo estratégico de la UE para que siga siendo un espacio abierto, garante de los derechos fundamentales y de la movilidad. La UE y los Estados miembros tienen la obligación de proteger la vida y la seguridad de todos los seres humanos; por lo tanto, el principio de no devolución debe respetarse plenamente.

1.3. Las medidas dirigidas a la interoperabilidad se comprenderán mejor si:

— garantizan, en el marco de la estrategia de la UE en materia de migración, las condiciones de equilibrio entre libertad y seguridad, en el respeto de la separación de poderes;

— garantizan a las personas afectadas sus derechos fundamentales, en particular la protección de sus datos personales y de su vida privada, el derecho de acceso a sus datos, a su rectificación y a su supresión en un plazo razonable, mediante procedimientos accesibles;

— reafirman, también en todos los textos de ejecución, la exigencia de integrar los principios de la protección de datos desde la fase de diseño;

— no crean nuevos obstáculos al tráfico normal de pasajeros y mercancías.

1.4. El CESE aboga por unos procedimientos y garantías respecto de la utilización de los datos para fines policiales que:

— prevean aplicar, en este ámbito, la legislación europea de mayor protección (el Reglamento general de protección de datos, RGPD);

— permitan acelerar la determinación del Estado miembro responsable del examen de las solicitudes de protección internacional;

— garanticen a las personas afectadas su derecho a dos niveles de jurisdicción;

— garanticen a los menores, en particular a los no acompañados, ya se encuentren en situación irregular, de persecución o delictiva, el derecho a obtener un visado, a estar protegidos e integrados y a beneficiarse del derecho al olvido en un plazo más breve que a los mayores.

1.5. El CESE considera que la base jurídica actual de los sistemas de información debería reforzarse y tener en cuenta la evolución de los sistemas de recopilación de datos. A este respecto, aboga por:

— reforzar la seguridad de las bases de datos existentes y de sus canales de comunicación;

— evaluar el impacto del refuerzo del control *a priori* sobre la gestión de riesgos;

— un control y evaluación permanentes de la arquitectura por parte de las autoridades de protección de datos (SEPD); por lo tanto, exige a los responsables que informen anualmente a las autoridades responsables de la toma de decisiones y a la Comisión sobre la seguridad de los componentes de interoperabilidad, y con carácter bienal respecto de las repercusiones de las medidas sobre los derechos fundamentales.

1.6. El CESE considera que el proyecto deberá contar con personal competente y es partidario de:

— programas sólidos de formación para las autoridades interesadas y los agentes de eu-LISA;

— un control estricto de las competencias de los agentes y candidatos para dicha agencia.

1.7. El CESE expresa su preocupación respecto de la financiación del nuevo sistema. El seguimiento de la planificación será fundamental para evitar desviaciones en los presupuestos y culminar el proyecto, hasta 2029.

1.8. El CESE recomienda que los ciudadanos sean informados de los avances del proyecto hasta su finalización y que las personas reciban una información pedagógica sobre los controles a los que están sujetas. Asimismo, considera que debe preverse la posibilidad de parar completamente el proyecto en caso de que la libertad y los derechos fundamentales estuvieran en peligro por un funcionamiento abusivo del sistema.

2. **Introducción**

2.1. En el contexto internacional de 2017, considerado inestable tanto desde el punto de vista geopolítico como en términos de seguridad interior de los Estados miembros, el Consejo pidió en varias ocasiones a la Comisión que instaurase los medios necesarios para localizar el paradero de personas consideradas «de riesgo» que ya hubieran sido fichadas en un Estado miembro. Detectar cuándo cruzan una frontera, sus viajes y trayectos en Europa podría ser crucial para la seguridad en la Unión.

2.2. En su Resolución de 6 de julio de 2016, el Parlamento pidió a la Comisión Europea que proporcionara las salvaguardias necesarias en materia de protección de datos.

2.3. Los textos examinados se incluyen en el objetivo sobre «la protección y el refuerzo de Schengen» ([1]). La Unión se ha dotado ya de varias normativas y servicios digitalizados de información en los ámbitos relacionados con el control del cruce de fronteras por parte de personas y mercancías.

2.4. Recordatorio:

— **SIS: Sistema de Información de Schengen**, uno de los mecanismos más antiguos, que ha sido revisado y gestiona un amplio abanico de alertas sobre personas y mercancías;

([1]) COM(2017) 570 final.

— **Eurodac: sistema europeo de comparación de impresiones dactilares** de los solicitantes de asilo y nacionales de terceros países en situación irregular en las fronteras y en los Estados miembros, y determinación del Estado miembro responsable de las solicitudes (CESE 2016-02981, ponente: Moreno Díaz) ([2]);

— **VIS: Sistema de Información de Visados** (Código de visados), que gestiona los visados para las estancias de corta duración (CESE 2014-02932, ponentes: Pezzini y Pariza Castaños) ([3]);

— **SES: Sistema de Entradas y Salidas**, actualmente a la espera de decisión, debería gestionar por vía electrónica los datos de los pasaportes y las fechas de entrada y salida de los nacionales de terceros países que visitan el espacio Schengen (CESE 2016-03098, SOC/544, ponente: Pîrvulescu) ([4]);

— **SEIAV: Sistema Europeo de Información y Autorización de Viajes**, en la actualidad a la espera de decisión, debería ser un gran sistema automatizado de almacenamiento y verificación *ex ante* de los datos de los nacionales de terceros países exentos de visado para circular en la zona Schengen (CESE 2016-06889, SOC/556, ponente: Simons) ([5]);

— **ECRIS-TCN: sistema europeo de intercambio de información sobre antecedentes penales de nacionales de terceros países**, en la actualidad propuesto por la Comisión, debería ser un sistema digital de intercambio de información sobre las resoluciones judiciales dictadas por los tribunales nacionales.

2.5. Se puede hacer la analogía entre los medios actuales de una autoridad facultada y un teléfono inteligente con distintas aplicaciones individuales, cada una de las cuales proporciona «su» información.

2.6. Salvo el SIS, estos sistemas se centran en la **gestión de los nacionales de terceros países**. Existen seis sistemas, complementarios y descentralizados. La información buscada es la suma de las respuestas obtenidas de las distintas bases por los servicios de investigación, en función de sus autorizaciones de acceso.

2.7. La Comisión quiere responder a la siguiente pregunta:

— ¿con qué método, sin cambiar las estructuras ya implantadas y conservando su complementariedad, se pueden poner todas las bases de datos en sintonía en el mismo momento para que, en un punto de entrada en el territorio europeo y mediante una sola consulta al sistema, converjan todos los datos recogidos en las bases existentes en la autoridad de control facultada para consultarlas, y todo ello respetando las normativas en materia de protección de datos y derechos fundamentales?

2.8. Con las propuestas objeto de examen, la Comisión Europea:

2.8.1. desea añadir las posibilidades adicionales que ofrecería un acceso a las bases de datos de Europol e Interpol, que cooperan ya con las autoridades de control europeas;

2.8.2. desea «sincronizar» las búsquedas de información para reducir los tiempos de respuesta por lo que respecta al expediente de los migrantes, así como acelerar la reacción de seguridad en caso necesario. Para ello, propone crear nuevas entidades que permitirían que las bases actuales funcionaran en simbiosis.

2.9. **Sus objetivos son: colmar en la mayor medida posible las lagunas de los distintos sistemas; mejorar la gestión** de las fronteras exteriores del espacio Schengen; contribuir a la seguridad interior de la Unión; gestionar los fraudes de identidad; resolver los casos de identidad múltiple; encontrar a personas sospechosas o ya condenadas y comprobar su identidad en el espacio Schengen.

2.10. Retomando la imagen del teléfono inteligente, la autoridad facultada no solo tendría a su disposición numerosas aplicaciones, sino que también podría recopilar de forma simultánea y en una misma búsqueda —utilizando sus códigos de acceso— los datos almacenados en todos sus soportes: PC, portátil, teléfono, tableta, *notebook*, etc.

([2]) DO C 34 de 2.2.2017, p. 144.
([3]) DO C 458 de 19.12.2014, p. 36.
([4]) DO C 487 de 28.12.2016, p. 66.
([5]) DO C 246 de 28.7.2017, p. 28.

3. **Funcionamiento del sistema**

3.1. La Comisión ha llevado a cabo consultas y ha reunido un Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad ([6]) designados por los Estados miembros, los países del Grupo Schengen y las agencias europeas, como eu-LISA ([7]) y FRA ([8]), bajo la coordinación de la DG HOME.

Método: ¿interconectividad o interoperabilidad?

3.1.1. La **interconectividad** de los sistemas de información es la posibilidad de conectarlos entre sí, de forma que los datos de uno puedan ser automáticamente consultados por otros.

3.1.2. La **interoperabilidad** ([9]) es la capacidad de distintos sistemas para comunicarse, intercambiar datos y utilizar la información intercambiada, respetando las autorizaciones de acceso a los sistemas.

3.2. *La elección de la interoperabilidad*

3.2.1. La Comisión considera que no trastoca los logros de las estructuras y competencias actuales y que los datos permanecerán en compartimentos estancos. A pesar del incremento de comunicabilidad, ello presentaría una ventaja de seguridad para los sistemas y los datos, ninguno de los cuales sería accesible evidentemente por internet. Los textos objeto del dictamen presentan importantes similitudes y tratan:

— uno, COM(2017) 793, de la interoperabilidad de los sistemas de información relativos a las fronteras y los visados,

— y el otro, COM(2017) 794, de la cooperación policial y judicial, asilo y migración.

3.3. *Las nuevas herramientas*

3.3.1. Para funcionar en la interoperabilidad, las seis bases se completarán con una nueva arquitectura de cuatro nuevas herramientas para trabajar rápidamente realizando una sola consulta al sistema, y manteniendo a las personas facultadas en el inicio de las solicitudes.

3.4. *El PEB (portal europeo de búsqueda)*

3.4.1. La autoridad de control facultada (el usuario final) debería disponer de un acceso único a todo el sistema. En lugar de efectuar seis búsquedas, solo lanzaría una (policía, aduana, etc.) para consultar simultáneamente varias bases sobre los datos buscados sin almacenar ninguno. Si existen, el sistema los encontrará. En caso de presunto delito o acto terrorista, la primera coincidencia puede ser neutra para la persona controlada («no-hit»), pero si el dato concuerda con una segunda información («hit») existente en bases como SIS, SES y SEIAV, ello podrá conducir a búsquedas más detalladas y a una investigación.

3.5. *El SCB compartido (servicio de correspondencia biométrica compartido)*

3.5.1. Esta plataforma compartida de correspondencia permitirá la búsqueda y comparación simultáneas de datos «matematizados», biométricos, impresiones dactilares y fotografías de identidad en las distintas bases, como SIS, Eurodac, VIS, *SES* ([10]), *ECRIS*, pero no *SEIAV*; sus datos deberán ser compatibles.

3.5.2. Por lo tanto, los datos «matematizados» no se conservarán en su forma original.

3.6. *El RCDI (registro común de datos de identidad)*

3.6.1. Un registro común de datos de identidad reunirá los datos relativos a la identidad biográfica y biométrica de los nacionales de terceros países controlados, ya se encuentren en la frontera o en los Estados miembros (de Schengen). Un indicador de concordancia de la información en las distintas bases acelerará la búsqueda. Bajo la responsabilidad y con los medios de seguridad de la Agencia eu-LISA, estos datos se salvaguardarán, de forma que ninguna persona pueda acceder a más de una línea alfanumérica a la vez. Desarrollado a partir del SES y del SEIAV, el RCDI no debería conducir a una duplicación de los datos. El repertorio podrá servir asimismo para búsquedas civiles.

([6]) DG HOME, Unidad B/3; Decisión de la Comisión C/2016/3780 de 17 de junio de 2016; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=EShttp://ec.europa.eu/transparency/regexpert/index.cfm?Lang=ES.

([7]) Agencia europea para la gestión operativa de los sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.

([8]) Agencia de los Derechos Fundamentales de la UE.

([9]) Comunicación de la Comisión COM(2016) 205 final, «Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad».

([10]) La cursiva recuerda que los textos relativos a esos sistemas todavía no se han adoptado.

3.7. *El DIM (detector de identidades múltiples)*

3.7.1. Verificará la correcta identidad de las personas de buena fe y combatirá los fraudes de identidad mediante una búsqueda en todas las bases al mismo tiempo. Este instrumento, que no ha sido utilizado todavía por ningún gobierno, debería permitir evitar la usurpación de identidad.

3.8. *Papel de la Agencia eu-LISA* ([11])

3.8.1. La Agencia, creada en 2011, tiene la misión de facilitar las políticas de la Unión en los ámbitos de la justicia, la seguridad y la libertad. Con sede en Tallin (Estonia), ya garantiza el intercambio de información entre las distintas fuerzas y cuerpos de seguridad de los Estados miembros y el funcionamiento sin discontinuidad de los sistemas informáticos de gran escala y la libertad de circulación de las personas en el espacio Schengen.

3.8.2. Trabaja en el proyecto «Fronteras inteligentes» y tendrá, en la nueva arquitectura de intercambios de datos, un papel de conservación de los elementos vinculados a las personas, así como de los relativos a las autoridades, las investigaciones y los investigadores. Controlará las autorizaciones de los solicitantes y garantizará la seguridad de los datos, también en caso «de incidente» [artículo 44 de las propuestas (2017) 793 y 794].

3.8.3. **La utilización del UMF (formato universal de mensajes)**, aún por crear, debería facilitar el trabajo con los nuevos sistemas, que serán obligatorios, al imponer la creación de interfaces en los Estados miembros que todavía carecen de ellas y un sistema de traducción temporal de una lengua a otra.

3.9. *La protección de los datos personales (artículos 7 y 8 de la Carta)*

3.9.1. La propuesta de Reglamento reconoce la posibilidad de incidentes de seguridad. Los Estados miembros y sus sistemas de datos deben ser los primeros en respetar los principios de protección de los datos previstos por los textos, el Tratado, la Carta de los Derechos Fundamentales y el RGPD ([12]), que entrará en vigor el 25 de mayo de 2018.

4. **Debate**

4.1. *Valor añadido de la interoperabilidad en democracia*

4.1.1. La UE necesita una regulación y unos medios de investigación que la protejan contra la delincuencia. La interoperabilidad de los sistemas de información es una oportunidad de hacer valer la primacía del Estado de Derecho y la defensa de los derechos humanos.

4.1.2. El *SES* y el *SEIAV*, en combinación con el SCB y el RCDI, permitirán controlar los cruces de las fronteras de las personas sospechosas y conservar sus datos. No obstante, la posibilidad de «acceso de los cuerpos policiales [por medio del SBC] a los sistemas de información no policiales a escala de la UE» (artículo 17/RCDI de las propuestas (2017) 793 y 794) no puede ser compatible con las finalidades enunciadas como bases de las propuestas objeto de examen. El Comité (artículo 300, apartado 4, del TFUE) debe mencionar aquí el principio de proporcionalidad y pide a la Comisión que evite cualquier programa tipo «gran hermano» ([13]) y crear obstáculos a la libertad de circulación de los ciudadanos europeos (artículo 3 del TUE).

4.1.3. El modelo propuesto para la recogida y la utilización de datos personales obtenidos en la frontera y dentro del territorio de la UE durante controles de desplazamientos y de documentos poseídos se presenta como estanco y abierto únicamente a personas autorizadas y para fines de seguridad y de gestión, aportando asimismo una mayor fluidez de los procedimientos.

4.1.4. El Comité tiene dudas acerca de la estanqueidad: quedarán lagunas, dado que la construcción planificada en nueve años se apoya sobre «cimientos» que todavía no existen, como los sistemas SES o SEIAV o las interfaces nacionales. El contexto tecnológico está en constante evolución, el proyecto se basa necesariamente en el estado de la técnica y no prevé en su presupuesto gestionar la obsolescencia que aparecería en determinados sectores digitales.

([11]) Reglamento (UE) n.º 1077/2011 del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.

([12]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Dictámenes del CESE: DO C 229 de 31.7.2012, p. 90 y DO C 345 de 13.10.2017, p. 138.

([13]) En la novela *1984*, de George Orwell.

4.1.5. Por otra parte, podría haberse considerado el desarrollo rápido de la utilización de algoritmos llamados de inteligencia artificial (IA) en el proyecto, simultáneamente como herramienta de control de los sistemas y como clave de seguridad confiada a las autoridades responsables para garantizar la utilización democrática de la arquitectura.

4.1.6. La propuesta desarrolla un sistema para personas de buena fe respetuosas de las leyes. El hecho de que haya personas al mando es reconfortante, pero también pueden constituir eslabones débiles. El Comité propone añadir un artículo que prevea «disyuntores» para los casos de crisis política o de «gestión», dado que cualquier problema en una base podría suponer un riesgo para toda la estructura ([14]). La generalización del UMF podría conducir a un uso internacional, muy positivo pero muy arriesgado para la protección de datos. Las autoridades facultadas asumirán una enorme responsabilidad. Estos aspectos no se abordan en los textos analizados.

4.2. *La protección de los derechos fundamentales*

4.2.1. Los derechos fundamentales son absolutos; solo se pueden introducir limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la UE y si se respeta su contenido esencial (artículo 8 y artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión). El Comité se pregunta cómo puede evaluarse la proporcionalidad de las medidas de control en el caso de migrantes que huyen de persecuciones y llegan a las costas de la UE [COM(2017) 794 final — Exposición de motivos — Derechos fundamentales]. La búsqueda de sospechosos con vistas a prevenir actos delictivos, en particular terroristas, **no debe aproximar a nuestras democracias al concepto de delito por anticipación**; debe existir una diferencia entre «actividades» que alteran el orden público y «opiniones».

4.2.2. El respeto de los derechos enunciados en la Carta para cualquier persona debe garantizar el equilibrio entre seguridad y libertad sin el cual la democracia muere. El Comité considera que este equilibrio es crucial y debe constituir un objetivo permanente para todas las autoridades, incluidas las autoridades de control nacionales y europeas.

4.2.3. La cadena de autoridades asociadas a una búsqueda, así como los metadatos correspondientes, se conservarán en el sistema. Se deben respetar los derechos fundamentales de las propias autoridades facultadas en relación con los datos generados, en particular en lo que se refiere a su seguridad y su vida privada, en caso de intrusión malintencionada en la estructura y de utilización indebida de los datos entre el momento de la obtención y aquel de su supresión.

4.3. *Protección de los datos*

4.3.1. Las propuestas reconocen el principio de la protección de datos desde la fase de diseño y por defecto, a pesar de que su exposición de motivos recuerde que, según el Tribunal de Justicia (TJUE), no se trata de una prerrogativa absoluta. El Comité reconoce las ventajas de medidas preventivas que garanticen la seguridad, de la lucha contra las identidades falsas y de la garantía del derecho de asilo. Sin embargo, desea subrayar los límites de la «matematización» y de la anonimización de los datos: las personas afectadas pueden necesitar sus datos posteriormente.

4.3.2. Asimismo, subraya que el tipo de datos conservados, biométricos y biológicos, reviste un especial interés para determinadas empresas y para la delincuencia. En este caso, la ciberseguridad es tan importante como la seguridad física, aunque se mencionada demasiado poco en las propuestas. Los datos conservados se almacenarán en un solo emplazamiento físico; incluso estando protegido, podría quedar expuesto.

4.3.3. El CESE recuerda que, en lo que se refiere a la protección de datos y al derecho de supresión (derecho al olvido), las instituciones y los órganos de la UE están sujetos al Reglamento (CE) n.º 45/2001, de menor protección que el RGPD ([15]) de 2016 (que entrará en vigor en mayo de 2018) que deben respetar los Estados miembros. El Comité subraya la complejidad de la aplicación de este derecho y duda de que los viajeros, migrantes y solicitantes de asilo estén en condiciones de hacer que se respete:

1) la protección de los datos personales debe estar validada por todas las bases existentes nacionales y europeas para que el conjunto esté protegido;

2) es fundamental para que los ciudadanos acepten esta inmensa red de vigilancia sobre sus cabezas.

4.3.4. En las propuestas no se especifica claramente la duración de la conservación de los datos recogidos por las autoridades facultadas. Los textos mencionan el procedimiento del derecho a rectificación o supresión, que tiene lugar entre el Estado miembro al que se haya realizado la solicitud y el Estado miembro responsable, pero no fijan una duración de la conservación de los datos (artículo 47 de las propuestas). El Comité pide que se fije dicho plazo y que este sea más corto para los menores (artículo 24 de la Carta), salvo en caso de terrorismo, de forma que estos puedan tener oportunidades de integrarse.

([14]) SEPD, anexo, informe final del Grupo de Expertos de Alto Nivel, mayo de 2017.
([15]) RGPD, Reglamento general de protección de datos [Reglamento (UE) 2016/679].

4.4. *Gobernanza y obligación de rendir cuentas*

4.4.1. Las bases de datos internacionales no están sujetas a las mismas normas que los sistemas informáticos europeos. El establecimiento de un formato universal de acceso, que podría tender a convertirse en internacional, será solo un elemento técnico que no unificará las normativas, aunque Interpol debe evidentemente respetar el artículo 17 del Pacto de las Naciones Unidas ([16]). Por otra parte, las autorizaciones seguirán siendo competencia de los Estados miembros. El CESE considera que debería abordarse este punto en las propuestas.

4.4.2. Una sola consulta, y la simbiosis de las bases europeas dará su veredicto. El CESE subraya que la burocracia generada será más que proporcional a la velocidad adquirida. La Comisión garantizará la gobernanza en el marco de un procedimiento de control con los Estados miembros. El eje será la Agencia eu-LISA, encargada en particular de establecer los procedimientos de recogida de información sobre el funcionamiento de la interoperabilidad; recibirá la información de los Estados miembros y de Europol y presentará cada cuatro años al Consejo, al Parlamento Europeo y a la Comisión un informe de evaluación técnica, y la Comisión preparará una valoración global un año más tarde (artículo 68 de las propuestas). Para el Comité, estas secuencias son demasiado largas. Debería realizarse una evaluación de la seguridad de los componentes de interoperabilidad [artículo 68, apartado 5, letra d)] al menos cada año y una evaluación de las repercusiones sobre los derechos fundamentales [ídem, letra b)] al menos cada dos años.

4.4.3. El Comité lamenta que cuestiones tan fundamentales como las que abordan estas propuestas sean gestionadas por agencias europeas, cuya contratación y funcionamiento resultan confusos para muchos ciudadanos. Considera necesario intercambiar buenas prácticas y asociar para conocer su opinión a todas las autoridades independientes de control de la utilización de los datos (SEPD) y a otras agencias como FRA y ENISA.

4.4.4. El establecimiento de todas estas nuevas estructuras y procedimientos se llevará a cabo mediante actos delegados y actos de ejecución de la Comisión. El Comité desearía que el objetivo de respetar los derechos fundamentales y de proteger los datos personales siga presente en todos estos actos a lo largo del tiempo, en un enfoque de mejora de la acogida a las personas en las fronteras. El CESE recomienda que los ciudadanos europeos sean informados de las etapas del proyecto hasta su finalización y que las personas reciban una información pedagógica sobre los controles a los que están sujetas.

5. **Las formaciones necesarias para las autoridades de control en toda la UE**

5.1. El Comité considera que serán necesarias numerosas formaciones durante el primer período (después de 2021), al contrario de lo que adelanta la Comisión en su resumen de la evaluación de impacto (C). Esta última menciona 76 millones EUR al año. La transición a nuevos procedimientos exige siempre un reajuste. Se trata, en este caso, de todas las fronteras de la UE y de los sistemas nacionales. Determinados Estados miembros aún no cuentan con sistemas compatibles y deberán realizar un esfuerzo importante para establecer interfaces que les permitan participar. Para que la interoperabilidad funcione, deberán reducirse las disparidades entre Estados miembros.

5.2. La formación en la utilización de datos de calidad y del UMF será fundamental. El Comité propone que se organice un centro de formación común para las autoridades facultadas, incluida la Agencia eu-LISA, en el que se verifiquen estrictamente las competencias de sus miembros, con la ayuda de CEPOL ([17]), Frontex, Europol, etc.

5.3. Una herramienta como el DIM no existe en ningún otro sitio. En caso de éxito, la herramienta será potente. La nueva arquitectura exigirá datos de la mejor calidad. Para que el conjunto esté a la altura de las expectativas del proyecto, todos los Estados miembros deben participar al mismo nivel, de lo contrario las lagunas serán más graves que antes. Y, en dicho caso, se debilitarían el derecho de asilo y el derecho de acceso a una protección internacional (artículos 18 y 19 de la Carta).

6. **La financiación**

6.1. Toda la arquitectura propuesta se basa sobre ciertas hipótesis: la adopción por las autoridades responsables de los sistemas *SES* y *SEIAV* y del *UMF*, el buen funcionamiento del *DIM* y la protección del *RCDI*. ¿Dispondrán dos organismos, el SEPD y la Agencia eu-LISA, a los que quizá se sume la Agencia ENISA, de suficientes medios personales y financieros? La Comisión propone una cofinanciación de la UE y los Estados miembros. El Comité observa que la gestión del «Semestre» se realiza todavía con presupuestos austeros y que, además, la utilización actual de las bases existentes (SIS, VIS, Prüm, *SES*) aún debe optimizarse en el respeto de los requisitos legales (informe del Grupo de Expertos).

([16]) Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas: «Artículo 17: 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques».

([17]) Agencia de la Unión Europea para la Formación Policial (Budapest, Hungría).

6.2. El CESE se pregunta por las repercusiones presupuestarias del *Brexit*, aunque el Reino Unido no esté en el sistema Schengen, y, más generalmente, sobre la futura complejidad de la gestión de la interoperabilidad en los países europeos no adscritos al SIS, pero participantes en otras bases, por ejemplo Eurodac.

6.3. El fondo previsto es el FSI, el Fondo de Seguridad Interior. El comienzo de la puesta en marcha se prevé para 2023. El Comité se pregunta si bastarán cinco años para reducir las disparidades europeas y gozar de condiciones para tener éxito. El presupuesto previsto es de 424,7 millones EUR a lo largo de un período de nueve años (2019-2027). Corresponderá a la UE (FSI) y a los Estados miembros pagar. Los Estados deben reunir las condiciones para hacer que los sistemas actuales funcionen correctamente con la nueva arquitectura informática. El Comité considera que la reactivación del crecimiento deberá servir para la realización de dichas inversiones.

Bruselas, 23 de mayo de 2018.

El Presidente
del Comité Económico y Social Europeo
Luca JAHIER