DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la cooperación administrativa a través del Sistema de Información del Mercado Interior («Reglamento IMI»)

(2012/C 48/02)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, el artículo 16,

Vista la Carta de los Derechos Fundamentales de la Unión Europea y, en particular, sus artículos 7 y 8,

Vista 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 ([1]),

Visto el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos ([2]),

Vista la solicitud de dictamen efectuada de conformidad con lo dispuesto en el artículo 28, apartado 2, del Reglamento (CE) nº 45/2001.

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1. INTRODUCCIÓN

1.1. Consulta al Supervisor Europeo de Protección de Datos

1. El 29 de agosto de 2011, la Comisión adoptó una propuesta de Reglamento (en adelante, «la propuesta» o «la propuesta de Reglamento») del Parlamento Europeo y del Consejo relativo a la cooperación administrativa a través del Sistema de Información del Mercado Interior (en adelante el «IMI») ([3]). Ese mismo día se dio traslado de la propuesta al SEPD para su consulta.

2. Antes de que fuera adoptada la propuesta, el SEPD tuvo oportunidad de formular observaciones a título informal sobre la misma, como había hecho anteriormente en relación con la Comunicación de la Comisión Mejorar la gobernanza del mercado único mediante una mayor cooperación administrativa: una estrategia para ampliar y desarrollar el Sistema de Información del Mercado Interior («IMI») (en adelante, «la Comunicación sobre la estrategia IMI») ([4]), antecedente de la propuesta. La propuesta ha tenido en cuenta muchas de las presentes observaciones, por lo que, en consecuencia, ha reforzado las garantías de protección de los datos.

3. El SEPD acoge con satisfacción el hecho de haber sido consultado a título informal por la Comisión, así como el hecho de que, en el preámbulo de la propuesta, se haya incluido una referencia al presente dictamen.

1.2. Objetivos y ámbito de aplicación de la propuesta

4. El IMI es una herramienta tecnológica de información que facilita a las autoridades competentes de los Estados miembros el intercambio recíproco de información en el momento de aplicar la legislación que regular el Mercado Interior. El IMI habilita una comunicación rápida y sencilla entre las autoridades locales, regionales y nacionales de los Estados miembros con sus homólogas de otros países europeos, lo que a su vez implica el tratamiento de los datos personales pertinentes, en particular información de carácter reservado.

5. En un principio, el IMI fue concebido como una herramienta de comunicación para los intercambios bilaterales en virtud de la Directiva de cualificaciones profesionales ([5]) y la Directiva sobre servicios ([6]). El IMI facilita a los usuarios la localización de la autoridad correspondiente de otro país con la que deben ponerse en contacto para comunicarse entre sí mediante un conjunto de preguntas y respuestas pre-traducidas ([7]).

([1]) DO L 281 de 23.11.1995, p. 31.
([2]) DO L 8 de 12.1.2001, p. 1.
([3]) COM(2011) 522 final.
([4]) COM(2011) 75.
([5]) Directiva 2005/36/CE del Parlamento Europeo y del Consejo, de 7 de septiembre de 2005, relativa al reconocimiento de cualificaciones profesionales (DO L 255 de 30.9.2005, p. 22).
([6]) Directiva 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios y el mercado interior (DO L 376 de 27.12.2006, p. 36).
([7]) Como ilustración de lo anterior, una pregunta habitual que incluye datos sensibles sería, por ejemplo: «¿Prueba jurídicamente el documento adjunto que no ha sido objeto de suspensión o prohibición del ejercicio de la profesión por falta profesional grave o infracción penal en relación con (el profesional migrante)?».

6. Ahora bien, el IMI aspira a convertirse en un sistema flexible y horizontal que sirva de apoyo a múltiples ámbitos normativos relacionados con el mercado interior. Está previsto ampliarlo gradualmente con el fin de apuntalar en el futuro otros ámbitos normativos.

7. También está previsto ampliar las aplicaciones del IMI. Además de los intercambios bilaterales de información, se prevén, o ya se han ejecutado, otras aplicaciones como los procedimientos de notificación, los mecanismos de alerta, los acuerdos de asistencia recíproca y la resolución de problemas ([8]) así como «un registro de información para referencia en el futuro por parte de los agentes del IMI» ([9]). Muchas de estas aplicaciones, aunque no todas, también pueden incluir el tratamiento de datos personales.

8. La propuesta tiene por objeto establecer un fundamento jurídico claro y un marco jurídico global para el IMI.

1.3. **Antecedentes de la propuesta: un enfoque gradual para establecer un marco global de protección de datos para el IMI**

9. Durante la primavera de 2007, la Comisión solicitó un dictamen del Grupo de Trabajo sobre protección de datos del Artículo 29 (en adelante, «el Grupo de Trabajo del Artículo 29») para que analizará las repercusiones del IMI en materia de protección de datos. El Grupo de Trabajo del Artículo 29 emitió un dictamen el 20 de septiembre de 2007 ([10]). en el que se recomendaba a la Comisión que clarificase el fundamento jurídico y brindase garantías específicas en materia de protección de datos para el intercambio de información a través del IMI. El SEPD participó activamente en las labores del subgrupo sobre el IMI y apoyó las conclusiones del dictamen del Grupo de Trabajo del Artículo 29.

10. Posteriormente, el SEPD proporcionó ulteriores orientaciones a la Comisión sobre cómo garantizar gradualmente un marco de protección de datos más global en el caso del IMI ([11]). En el marco de esta cooperación, y desde que el 22 de febrero de 2008 formulase su dictamen sobre la explotación del IMI ([12]), el SEPD no ha dejado de insistir en la necesidad de un nuevo instrumento jurídico aprobado mediante el procedimiento legislativo ordinario, con el fin de instaurar un marco de protección de datos más exhaustivo en el caso del IMI y brindar seguridad jurídica. La propuesta correspondiente a dicho instrumento jurídico se presenta en este momento ([13]).

([8]) Véase el considerando 10.

([9]) Véase el artículo 13, apartado 2.

([10]) Dictamen nº 7/2007 del Grupo de Trabajo sobre Protección de Datos del Artículo 29 sobre cuestiones de protección de datos relacionadas con el Sistema de Información del Mercado Interior (IMI), WP140. Disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp140_es.pdf

([11]) Los documentos clave relativos a esta cooperación están disponibles en el sitio web sobre el IMI de la Comisión http://ec.europa.eu/internal_market/imi-net/data_protection_es.html, así como en el sitio web del SEPD http://www.edps.europa.eu

([12]) Dictamen del Supervisor Europeo de Protección de Datos sobre la Decisión 2008/49/CE de la Comisión, de 12 de diciembre de 2007, relativa a la protección de los datos personales en la explotación del Sistema de Información del Mercado Interior (IMI), por lo que se refiere a la protección de los datos personales (DO C 270 de 25.10.2008, p. 1).

([13]) El Grupo de Trabajo del Artículo 29 también tiene planeado comentar la propuesta. El SEPD ha seguido esta evolución en el correspondiente subgrupo del Grupo de Trabajo del Artículo 29 en el que ha aportado sus observaciones.

2. **ANÁLISIS DE LA PROPUESTA**

2.1. **Dictamen general del SEPD sobre la propuesta y sobre las principales dificultades que comporta la regulación del IMI**

11. El dictamen del SEPD sobre el IMI es en general positivo. El SEPD respalda los objetivos de la Comisión de instaurar un sistema electrónico de intercambio de información y de regular aquellos aspectos del sistema relacionados con la protección de datos. Un sistema racionalizado de estas características no solo contribuiría a una cooperación más eficiente, sino que como efecto derivado también garantizaría el cumplimiento de la normativa aplicable en materia de protección de datos, ya que aportaría un marco claro en relación con el tipo de información que es posible intercambiar, con quién y en qué condiciones.

12. El SEPD acoge asimismo con agrado el hecho de que la Comisión proponga en el caso del IMI un instrumento jurídico horizontal en forma de Reglamento del Parlamento Europeo y del Consejo. Al SEPD le complace que la propuesta acentúe en general los puntos más relevantes que atañen a la protección de datos dentro del IMI. Sus observaciones deben ser leídas y cotejadas a la luz de estos antecedentes positivos.

13. Sin embargo, el SEPD advierte que el establecimiento de un único sistema electrónico centralizado para los múltiples ámbitos de la cooperación administrativa también comporta riesgos. Entre ellos, en particular, el hecho de que se incrementaría el número de datos compartidos, en términos más amplios de los estrictamente necesarios a efectos de una cooperación eficaz, y que los datos, en particular los potencialmente obsoletos e inexactos, podrían permanecer en el sistema electrónico más tiempo del necesario. La seguridad del sistema de información al que es posible acceder en los 27 Estados miembros también es una cuestión delicada, puesto que la seguridad del sistema en conjunto estará únicamente en función del nivel de seguridad en el eslabón más débil de la cadena.

Principales retos

14. Por lo que se refiere al marco jurídico para el IMI que es preciso establecer en el Reglamento propuesto, el SEPD llama la atención sobre dos dificultades principales:

— la necesidad de garantizar la coherencia, al tiempo que se respeta la diversidad, y

— la necesidad de equilibrio entre la flexibilidad y la seguridad jurídica.

15. Estas dificultades primordiales sirven como importantes puntos de referencia y determinan, en gran medida, el enfoque adoptado por el SEPD en el presente dictamen.

Coherencia al tiempo que se respeta la diversidad

16. En primer lugar, el IMI es un sistema utilizado en 27 Estados miembros. En el estado actual de armonización de las legislaciones europeas, existen diferencias sustanciales entre los procedimientos administrativos empleados a nivel nacional, así como entre las legislaciones nacionales en materia de protección de datos. El IMI debe articularse de tal modo que los usuarios en cada uno de los 27

Estados miembros puedan respetar sus legislaciones nacionales, en particular la legislación nacional en materia de protección de datos, cuando intercambien datos personales a través del IMI. A la vez, es preciso asegurar a los interesados que sus datos serán protegidos coherentemente, al margen de que a través del IMI se transmitan datos a otro Estado miembro. La coherencia, respetando al mismo tiempo la diversidad, es un problema importante a la hora de construir tanto la infraestructura técnica como la infraestructura jurídica del IMI. Ha de evitarse una complejidad y una fragmentación indebidas. El tratamiento de datos en el seno del IMI debe ser transparente y las responsabilidades en materia de toma de decisiones relativas al diseño del sistema, su mantenimiento y uso diarios, así como su supervisión, deben estar claramente atribuidas.

Equilibrio entre flexibilidad y seguridad jurídica

17. En segundo lugar, a diferencia de otros sistemas informáticos a gran escala, como el Sistema de Información de Schengen, el Sistema de Información de Visados, el Sistema de Información Aduanero o Eurodac, orientados a la cooperación en ámbitos específicos y claramente definidos, el IMI es una herramienta horizontal de intercambio de información y puede ser utilizada para facilitar el intercambio de información en muchos ámbitos políticos diferentes. También está previsto ampliar gradualmente el ámbito de aplicación del IMI hacia otros ámbitos políticos y que sus aplicaciones puedan ser modificadas a fin de dar cabida a otros tipos de cooperación administrativa hasta hoy no especificados. Estos rasgos característicos del IMI se traducen en una mayor dificultad a la hora de definir con claridad las aplicaciones del sistema y los intercambios de datos que podría generar. Por lo tanto, definir claramente garantías adecuadas para la protección de datos resulta aún más problemático.

18. El SEPD reconoce la necesidad de flexibilidad y toma nota de la voluntad de la Comisión de lograr que el Reglamento «resista el paso del tiempo». No obstante, esto no debería comportar una falta de claridad y de seguridad jurídica en cuanto a las aplicaciones del sistema y las garantías que en materia de protección de datos es preciso implantar. Por este motivo, y en la medida de lo posible, la propuesta ha de ser más específica y no limitarse únicamente a reiterar los principios fundamentales que en materia de protección de datos establecen la Directiva 95/46/CE y el Reglamento (CE) nº 45/2001 ([14]).

2.2. **Ámbito de aplicación del IMI y ampliación prevista (artículos 3 y 4)**

2.2.1. *Introducción*

19. El SEPD acoge con satisfacción la claridad con que se define en la propuesta el ámbito de aplicación actual del IMI, junto con el anexo I en el que se recoge un listado de los actos relevantes de la Unión, en base a los cuales es posible el intercambio de información. Dicho listado incluye la cooperación en virtud de las disposiciones específicas de la Directiva relativa a las cualificaciones profesionales, la Directiva de servicios y la Directiva relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza ([15]).

20. Dado que está previsto ampliar el ámbito de aplicación del IMI, en el anexo II se incorpora un listado de los posibles objetivos de la ampliación. Los elementos del anexo II pueden trasladarse al anexo I mediante un acto delegado que deberá ser adoptado por la Comisión, una vez efectuada una evaluación de impacto ([16]).

21. El SEPD acoge con satisfacción esta técnica ya que i) delimita claramente el ámbito de aplicación del IMI y ii) garantiza la transparencia, iii) permitiendo al mismo tiempo flexibilidad en los casos en que se utilice el IMI para intercambios de información adicionales en el futuro. Asimismo, también garantiza que no se lleva a cabo ningún intercambio de información a través del IMI sin i) contar con un fundamento jurídico adecuado en la normativa específica sobre mercado interior que autorice o instruya el intercambio de información ([17]), e ii) incluir una referencia a dicha base jurídica en el anexo I del Reglamento.

22. Dicho esto, subsiste la incertidumbre, en relación con el ámbito de aplicación del IMI, por lo que se refiere a los ámbitos políticos en los que es posible proceder a la ampliación del IMI, y a las aplicaciones que están o pueden tener cabida dentro del IMI.

23. En primer lugar, no cabe excluir que el ámbito de aplicación del IMI pueda ampliarse más allá de los ámbitos políticos contemplados en las listas del anexo I y del anexo II. Tal podría ser el caso si el IMI se emplease para determinados tipos de intercambio de información no en un acto delegado de la Comisión sino en un acto adoptado por el Parlamento y el Consejo en el caso de que esto no esté previsto en el anexo II ([18]).

([14]) En este sentido, véanse nuestros comentarios en el apartado 2.2 en relación con la ampliación prevista del IMI.

([15]) Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa al reconocimiento de cualificaciones profesionales (DO L 88 de 4.4.2011, p. 45).

([16]) El propio proyecto de Reglamento no hace referencia a la evaluación de impacto. Sin embargo, en la página 7 de la Exposición de motivos de la propuesta se explica que la Comisión podrá trasladar elementos del anexo II al anexo I, adoptando un acto delegado y «tras una evaluación de la viabilidad técnica, la relación coste-eficacia, la facilidad de uso y la repercusión general sobre el sistema, así como, en su caso, de los resultados de una posible fase de pruebas».

([17]) Lo anterior se entiende a excepción de SOLVIT (véase el anexo II, apartado I, punto 1), en la que únicamente está disponible una «regla no vinculante», una Recomendación de la Comisión. Desde el punto de vista de la protección de datos, en opinión del SEPD, en el caso específico del SOLVIT, la base jurídica del tratamiento puede ser el «consentimiento» de los interesados.

([18]) Esto puede ocurrir a iniciativa de la Comisión aunque tampoco puede quedar excluido que la idea de utilizar el IMI en un ámbito político específico pueda aparecer posteriormente en el proceso legislativo, y también puede ser propuesta por el Parlamento o por el Consejo. Esto también había ocurrido en el pasado respecto de la Directiva relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza. En tal caso, se exigiría más claridad en relación con el «procedimiento» de ampliación que parece haberse centrado únicamente en el supuesto de ampliación mediante actos delegados (véanse las disposiciones relativas a la evaluación de impacto, actos delegados, actualización del anexo I).

24. En segundo lugar, aunque extender el ámbito de aplicación a nuevos ámbitos políticos podría en algunos casos no requerir ningún cambio o pocos cambios de las aplicaciones existentes del sistema ([19]), otras ampliaciones podrían requerir aplicaciones nuevas y diferentes, o cambios importantes en las aplicaciones existentes:

— aunque la propuesta hace referencia a diversas funcionalidades existentes o previstas, dichas referencias no son lo suficientemente claras o no están lo suficientemente detalladas. Ello es aplicable, en diferente medida, a las referencias a alertas, agentes externos, registros, acuerdos de asistencia recíproca y resolución de problemas ([20]). Como ejemplo de todo lo anterior, el término «alerta», que se refiere a una aplicación existente y esencial se menciona una sola vez, en el considerando 10,

— en virtud de la propuesta de Reglamento, es posible adoptar nuevos tipos de aplicaciones que en la propuesta no se mencionan en absoluto,

— hasta ahora ha venido describiéndose el IMI como una herramienta informática de intercambio de información, o en otras palabras, una herramienta de comunicación (véase, por ejemplo, el artículo 3 de la propuesta). Sin embargo, algunas de las aplicaciones mencionadas en la propuesta, en particular la función de «registro de información», parecen trascender este concepto. La propuesta de ampliación a cinco años de los períodos de conservación también parece indicar el paso hacia una «base de datos». Estas evoluciones alterarían fundamentalmente el carácter del IMI ([21]).

2.2.2. *Recomendaciones*

25. Para solventar estas incertidumbres, el SEPD recomienda un enfoque a dos niveles. En primer lugar, propone que las aplicaciones ya previsibles se clarifiquen y se aborden de manera más detallada; y en segundo lugar, que se apliquen las adecuadas garantías de procedimiento con el fin de velar por que la protección de los datos sea minuciosamente tenida en cuenta en la futura evolución del IMI.

Aclaración de las aplicaciones ya disponibles o previsibles (por ejemplo, los intercambios bilaterales, las alertas, los registros, la resolución de problemas y los agentes externos)

26. El SEPD recomienda que el Reglamento especifique más claramente las aplicaciones cuando ya sean conocidas, como es el caso de los intercambios de información mencionados en los anexos I y II.

27. Por ejemplo, podrían preverse medidas más claras y específicas para la integración de SOLVIT ([22]) en el IMI (disposiciones sobre «agentes externos» y «resolución de problemas») y para los directorios de profesionales y proveedores de servicio (disposiciones relativas a los «registros»).

28. También deben formularse aclaraciones adicionales en relación con las «alertas», que se emplean ya en virtud de la Directiva de servicios y que también pueden introducirse en otros ámbitos políticos. En particular, la «alerta» como funcionalidad debe definirse claramente en el artículo 5 (junto con otras aplicaciones, como los intercambios de información individuales y los registros). Los derechos de acceso y los períodos de conservación para las alertas deben ser aclarados ([23]).

Garantías de procedimiento (evaluación de impacto sobre la protección de datos y consulta a las autoridades competentes en materia de protección de datos)

29. Si la intención es que el Reglamento «resista el paso del tiempo» por lo que se refiere a las aplicaciones adicionales que puedan resultar necesarias a largo plazo y, de este modo, permitir otras aplicaciones todavía no definidas en el Reglamento, esto debe ir acompañado de las garantías de procedimiento adecuadas que aseguren la adopción de las disposiciones apropiadas para implantar las necesarias garantías en materia de protección de datos antes de proceder al despliegue de una nueva aplicación. Lo mismo sería válido para las ampliaciones a nuevos ámbitos políticos en los que ello repercutiría sobre la protección de datos.

30. El SEPD recomienda un mecanismo claro que garantice que con antelación a cada ampliación de las aplicaciones, o ampliaciones a nuevos ámbitos políticos, se evalúen cuidadosamente las cuestiones relativas a la protección de datos y, en su caso, se implanten las garantías o medidas técnicas adicionales en la arquitectura del IMI. En especial:

— la evaluación de impacto a que se hace referencia en la página 7 de la exposición de motivos debe requerirse específicamente en el propio Reglamento y también debe incluirse una evaluación de impacto sobre la protección de datos, en la que debe abordarse específicamente qué modificaciones son necesarias, en su caso, en el diseño del IMI a fin de garantizar que continúe incluyendo las adecuadas garantías de protección de datos que cubren también los nuevos ámbitos políticos o aplicaciones,

— el Reglamento debe establecer específicamente que, antes de cada ampliación del IMI, será obligatoria la consulta al SEPD y a las autoridades nacionales responsables de la protección de datos. Esta consulta puede llevarse a cabo a través del mecanismo previsto para la supervisión coordinada contemplado en el artículo 20.

([19]) Por ejemplo, los intercambios de información bilaterales en virtud de la Directiva relativa a cualificaciones profesionales y la Directiva relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza se atienen fundamentalmente a la misma estructura y pueden adaptarse utilizando aplicaciones similares, con sujeción a similares garantías en materia de protección de datos.

([20]) Véanse los considerandos, 2, 10, 12, 13 y 15, y el artículo 5, letras b) e i), el artículo 10, apartado 7, y el artículo 13, apartado 2.

([21]) Incidentalmente, si existe la intención de que el IMI sustituya/complemente los sistemas de gestión y archivo de ficheros, o que el mismo se utilice como base de datos, esto debería clarificarse mejor en el artículo 3.

([22]) Véase el anexo II, apartado I, punto 1.

([23]) Véanse los apartados 2.4. y 2.5.5. *infra*.

31. Estas garantías de procedimiento (la evaluación de impacto sobre la protección de datos y la consulta) deben ser aplicables a la ampliación tanto mediante un acto delegado de la Comisión (trasladando un elemento del anexo II al anexo I) como a través de un Reglamento del Parlamento Europeo y del Consejo, en particular aquel elemento no incluido en la lista del anexo II.

32. Por último, el SEPD recomienda que el Reglamento clarifique si el ámbito de aplicación de los actos delegados que la Comisión estará facultada para adoptar con arreglo al artículo 23 incluirá cualquier otra cuestión aparte el traslado de elementos del anexo II al anexo I. Si fuera viable, el Reglamento deberá facultar a la Comisión para adoptar actos de ejecución o delegados específicos con el fin de definir mejor cualquier funcionalidad adicional del sistema o solventar cualquier problema que en materia de protección de datos pueda plantearse en el futuro.

2.3. **Funciones, competencias y responsabilidades (artículos 7 a 9)**

33. El SEPD acoge con satisfacción que se haya consagrado todo un capítulo (capítulo II) a aclarar las funciones y las responsabilidades de los distintos agentes implicados en el IMI. Las disposiciones podrían reforzarse en los siguientes términos.

34. El artículo 9 describe las responsabilidades inherentes a la función de la Comisión en tanto que responsable del tratamiento. El SEPD recomienda asimismo incluir una disposición adicional relativa a la función de la Comisión como garante de que el sistema aplica en su concepción los principios de «protección de la intimidad incorporada el diseño», así como a su función de coordinación respecto de las cuestiones en materia de protección de datos.

35. Al SEPD le complace que las tareas de los coordinadores del IMI incluidas en el artículo 7 ahora incluyan específicamente las tareas de coordinación relativas a la protección de datos, incluyendo actuar como persona de contacto con la Comisión. Recomienda que se aclare con más detalle que estas tareas de coordinación también incluyen los contactos con las autoridades nacionales encargadas de la protección de datos.

2.4. **Derechos de acceso (artículo 10)**

36. El artículo 10 establece garantías en relación con los derechos de acceso. El SEPD acoge con satisfacción el hecho de que, tras sus observaciones, estas disposiciones se hayan visto significativamente reforzadas.

37. Considerando el carácter horizontal y expansivo del IMI, resulta importante asegurar que el sistema garantice la aplicación de «muros protectores» que limiten la información exclusivamente tratada en un ámbito político a dicho ámbito: los usuarios del IMI solo deben i) acceder a la información cuando precisen conocerla y ii) dicha información se limitará a un único ámbito político.

38. Si un usuario del IMI estuviese inevitablemente facultado para acceder a la información relativa a diversos ámbitos políticos (como puede ser el caso, por ejemplo, de determinados departamentos del gobierno local), como mínimo, el sistema no deberá permitir la combinación de información procedente de diferentes ámbitos políticos. Deben establecerse, de ser necesarias, excepciones en la aplicación de la legislación o en un acto de la Unión, observando estrictamente el principio de limitación a una finalidad específica.

39. Estos principios están actualmente esbozados en el texto del Reglamento pero podrían reforzarse y hacerse más operativos.

40. En relación con los derechos de acceso por parte de la Comisión, el SEPD acoge con satisfacción el hecho de que el artículo 9, apartados 2 y 4, y el artículo 10, apartado 6, de la propuesta, considerados en conjunto, especifiquen que la Comisión no tendrá acceso a los datos personales intercambiados entre los Estados miembros, salvo en los casos en que se designe a la Comisión como parte en un procedimiento de cooperación administrativa.

41. Los derechos de acceso por parte de los agentes externos y el derecho de acceso a las alertas también deberán especificarse con mayor claridad ([24]). En este sentido, el SEPD recomienda que en el Reglamento se establezca que las alertas no deben ser enviadas, por defecto, a todas las autoridades competentes relevantes en todos los Estados miembros sino sólo a las que resultan afectadas, y únicamente cuando deban conocerlas. Esto no excluye enviar alertas a todos los Estados miembros en casos específicos o en ámbitos políticos específicos, si todos resultan afectados. De manera similar, los análisis caso por caso son necesarios para determinar si la Comisión ha de tener acceso a las alertas.

2.5. **Conservación de los datos personales (artículos 13 y 14)**

2.5.1. *Introducción*

42. El artículo 13 de la propuesta amplía la duración del período de almacenamiento de datos dentro del IMI desde los actuales seis meses (que deben contarse a partir del momento en que se archiva el asunto) hasta los cinco años, quedando «bloqueados» los datos al cabo de dieciocho meses. Durante el período de «bloqueo», los datos únicamente serán accesibles a través de un procedimiento específico de recuperación, que únicamente podrá ser iniciado a petición del interesado o en el supuesto de que los datos sean necesarios «a efectos probatorios de un intercambio de información a través del IMI».

43. En efecto, de este modo, los datos se almacenan en el IMI durante tres períodos diferenciados:

— desde el momento de la carga hasta el momento en que se archiva el asunto,

— desde que se archiva el asunto y durante un período de dieciocho meses ([25]),

— desde el transcurso del período de 18 meses, de manera bloqueada, durante otro período de tres años y seis meses (dicho de otro modo, hasta que hayan transcurridos cinco años desde el archivo del asunto).

([24]) Véase asimismo el apartado 2.2.2.

([25]) El artículo 13, apartado 1, indica que dieciocho meses es un plazo «máximo», pudiendo ser establecido, por tanto, un período más corto. Esto, sin embargo, no tendría efectos sobre la duración total de la conservación que podría prolongarse, en cualquier caso, hasta el final de los cinco años desde el archivo del asunto.

44. Más allá de estas normas generales, el artículo 13, apartado 2, permite conservar los datos en un «registro de información» mientras sea necesaria a estos efectos, con el consentimiento del interesado o cuando «sea necesario para dar cumplimiento a un acto jurídico de la Unión». Además, el artículo 14 establece un mecanismo de bloqueo similar para la conservación de los datos personales de los usuarios del IMI, durante cinco años, desde la fecha en que un usuario causa baja en el IMI.

45. No existen otras disposiciones específicas al respecto. Por lo tanto, presumiblemente, las normas generales están destinadas a ser aplicadas no solo a los intercambios bilaterales sino también a las alertas, la resolución de problemas [como en SOLVIT ([26])] y a todo el resto de aplicaciones que implican un tratamiento de datos personales.

46. El SEPD manifiesta varias inquietudes en relación con los períodos de conservación, a la luz de lo dispuesto en el artículo 6, apartado 1, letra e), de la Directiva 95/46/CE y el artículo 4, apartado 1, letra e), del Reglamento (CE) nº 45/2011, que exigen que los datos personales deban ser conservados durante un período que no podrá exceder al necesario para la consecución de los fines para los que fueron recabados o para los que se traten posteriormente.

2.5.2. *Desde la carga hasta el archivo del asunto: la necesidad del oportuno archivo del asunto*

47. En relación con el primer período, desde la carga de la información hasta el archivo del asunto, al SEPD le preocupa el riesgo de que algunos asuntos puedan no llegar cerrarse o cerrarse únicamente al cabo de un período desproporcionadamente largo. Esto puede conducir a que algunos datos personales permanezcan en la base de datos más de lo necesario o indefinidamente.

48. El SEPD entiende que la Comisión ha hecho progresos, a nivel práctico, para reducir los asuntos pendientes en el IMI y que existe un sistema para los intercambios bilaterales destinado a controlar oportunamente los asuntos archivados y recordar periódicamente los casos pendientes. Además, un nuevo cambio en las aplicaciones del sistema, conforme a un enfoque de «protección de la intimidad incorporada en el diseño», permite, con sólo pulsar un botón, aceptar una respuesta y, al mismo tiempo, dar por cerrado el asunto. Anteriormente, esto exigía llevar a cabo dos pasos independientes y podía conducir a que algunos casos inactivos permanecieran en el sistema.

49. El SEPD acoge con satisfacción los esfuerzos realizados a nivel práctico. Sin embargo, recomienda que el texto del propio Reglamento establezca garantías de que los asuntos se archivarán oportunamente en el IMI y que los asuntos inactivos (casos sin ninguna actividad reciente) serán eliminados de la base de datos.

2.5.3. *Desde el archivo del asunto hasta los dieciocho meses: ¿está justificada la ampliación del período de seis meses?*

50. El SEPD invita a reconsiderar si existe una justificación adecuada para ampliar el actual período de seis meses tras el archivo del asunto y, en tal caso, si la justificación es aplicable únicamente a los intercambios de información bilaterales o también a otros tipos de aplicaciones. En la actualidad, el IMI ya cuenta con varios años de existencia y debería aprovecharse la experiencia práctica acumulada en este sentido.

51. Si el IMI sigue siendo un herramienta para el intercambio de información (en contraposición con un sistema de gestión de archivos, una base de datos o un sistema de archivo) y se establece además que se proporcionará a las autoridades competentes medios para extraer la información que obtienen del sistema (ya sea en forma electrónica o en papel, pero en cualquier caso, de modo que puedan utilizar la información extraída con carácter de prueba ([27])), no parece haber ninguna necesidad de conservar los datos en el IMI una vez archivado el asunto.

52. En los intercambios de información bilaterales, la necesidad potencial de formular preguntas de seguimiento incluso después de haber aceptado una respuesta y, por tanto, haber archivado un asunto, quizás pueda justificar un período (razonablemente corto) de conservación tras el archivo del asunto. El actual período de seis meses parece a priori lo suficientemente generoso a estos efectos.

2.5.4. *Desde los dieciocho meses hasta los cinco años: datos «bloqueados»*

53. El SEPD considera que la Comisión tampoco ha justificado suficientemente la necesidad y la proporcionalidad de la conservación de los «datos bloqueados» hasta un período de cinco años.

54. La exposición de motivos, en la página 8, hace referencia a la sentencia *Rijkeboer* ([28]) del Tribunal de Justicia. El SEPD recomienda a la Comisión que reconsidere las implicaciones de dicho asunto sobre la conservación de datos en el IMI. En su opinión, el asunto *Rijkeboer* no exige configurar el IMI para conservar datos durante cinco años tras el archivo del asunto.

55. El SEPD no considera que la referencia a la sentencia *Rijkeboer* o a los derechos de los interesados de tener acceso a sus datos constituya una justificación suficiente y adecuada para conservar los datos en el IMI durante cinco años tras el archivo del asunto. La conservación únicamente de los «datos de registro» (estrictamente definidos para excluir cualquier contenido, entre otros, cualquier archivo adjunto o dato sensible) puede ser una opción menos imprudente que podría ser merecedora de mayor consideración. Sin embargo, en la presente fase, el SEPD no está convencido de que incluso eso fuera necesario o proporcionado.

([26]) Véase el anexo II, apartado I, punto 1.

([27]) Entendemos que se han llevado a cabo esfuerzos para garantizar esto a nivel práctico.

([28]) C-553/07 *Rijkeboer* [2009] Recopilación de Jurisprudencia I-3889.

56. Además, la falta de claridad sobre quién puede tener acceso a los «datos bloqueados» y para qué fines también plantea problemas. La simple referencia al uso «a efectos probatorios de un intercambio de información» (tal como dispone el artículo 13, apartado 3) no es suficiente. Si se conserva la disposición relativa al «bloqueo», en cualquier caso, debe especificarse mejor quién puede solicitar la prueba de un intercambio de información y en qué contexto. Además del interesado, ¿qué otras personas pueden solicitar el acceso? En ese caso, ¿serían éstas las únicas autoridades competentes y el acceso sería únicamente para probar que ha tenido lugar un intercambio de información particular con un determinado contenido (en el caso de que dicho intercambio sea impugnado por las autoridades competentes que enviaron o recibieron el mensaje)? ¿Se han previsto otros posibles usos «a efectos probatorios de un intercambio de información»? ([29])

2.5.5. *Alertas*

57. El SEPD recomienda establecer una diferencie más clara entre las alertas y los registros de información. Una cosa es utilizar una alerta como herramienta de comunicación para avisar a las autoridades competentes sobre una irregularidad o sospecha particular y otra almacenar dicha alerta en una base de datos durante un período amplio o incluso indefinido. Almacenar información sobre alertas plantearía otras inquietudes y exigiría normas específicas y garantías adicionales de protección de datos.

58. Por lo tanto, el SEPD recomienda que el Reglamento establezca, como norma por defecto que i) —salvo especificación en contrario en la normativa vertical y con sujeción a las adecuadas garantías adicionales— se aplique un período de conservación de seis meses a las alertas y, lo que es más importante, que ii) dicho período empiece a contabilizarse a partir del momento en que se envía la alerta.

59. De manera alternativa, el SEPD recomienda que el Reglamento propuesto establezca específicamente garantías detalladas en relación con las alertas. Si se sigue este segundo enfoque, el SEPD está dispuesto a ayudar a la Comisión y a los legisladores ofreciéndoles asesoramiento en este sentido.

2.6. **Categorías especiales de datos (artículo 15)**

60. El SEPD acoge con satisfacción la distinción efectuada entre, por un lado, los datos personales mencionados en el artículo 8, apartado 1, de la Directiva 95/46/CE, y los datos personales mencionados en el artículo 8, apartado 5, por otro. También acoge con satisfacción que el Reglamento especifique claramente que las categorías especiales de datos únicamente pueden ser tratadas sobre la base del motivo específico mencionado en el artículo 8 de la Directiva 95/46/CE.

61. En este sentido, el SEPD entiende que el IMI tratará una cantidad significativa de datos sensibles inscritos en el ámbito del artículo 8, apartado 2, de la Directiva 95/46/CE. De hecho, el IMI, desde sus inicios, cuando se desplegó por primera vez con el fin de contribuir a la cooperación administrativa en virtud de la Directiva de servicios y la Directiva relativa a cualificaciones profesionales, fue concebido para tratar dichos datos, en particular, datos relativos a los registros de infracciones penales y administrativas que pudieran afectar al derecho del profesional o del proveedor de servicios a prestar sus servicios o desarrollar su trabajo en otro Estado miembro.

62. De manera adicional, también cabe la posibilidad de que el IMI trate una cantidad significativa de datos sensibles en virtud del artículo 8, apartado 1 (principalmente relacionados con la salud), una vez que el IMI sea ampliado con el fin de dar cabida a un módulo para SOLVIT ([30]). Por último, no se debe ignorar que a través del IMI también podrán obtenerse en el futuro otros datos sensibles, de manera sistemática o puntual.

2.7. **Seguridad (artículo 16 y considerando 16)**

63. Al SEPD le complace observar que el artículo 16 incluye una referencia específica a la obligación de la Comisión de seguir sus propias normas internas, adoptadas con el fin de ajustarse a lo dispuesto en el artículo 22 del Reglamento (CE) nº 45/2001 y para adoptar y mantener actualizado el plan de seguridad del IMI.

64. Para reforzar estas disposiciones, el SEPD recomienda que el Reglamento exija una evaluación del riesgo y una revisión del plan de seguridad antes de cada ampliación del IMI a un nuevo ámbito político o antes de añadir una nueva aplicación que repercuta sobre los datos personales ([31]).

65. Además, el SEPD señala asimismo que el artículo 16 y el considerando 16 solo hacen referencia a las obligaciones de la Comisión y a la función supervisora del SEPD. Esta referencia puede resultar engañosa. Aunque es verdad que la Comisión es el operador del sistema y que, como tal, es responsable de la mayor parte del mantenimiento de la seguridad del IMI, a las autoridades competentes también se les reservan obligaciones que, a su vez, están supervisadas por las autoridades nacionales competentes en materia de protección de datos. Por lo tanto, el artículo 16 y el considerando 16 también deben hacer referencia a las obligaciones en materia de seguridad aplicables al resto de agentes del IMI, en virtud de lo dispuesto en la Directiva 95/46/CE y de las competencias de supervisión de las autoridades nacionales competentes en materia de protección de datos.

2.8. **Información a los interesados y transparencia (artículo 17)**

2.8.1. *Información proporcionada en los Estados miembros*

66. En relación con el artículo 17, apartado 1, el SEPD recomienda añadir algunas disposiciones más específicas en el Reglamento con el fin de garantizar a los interesados el derecho a estar plenamente informados sobre el tratamiento que le da a sus datos en el IMI. Considerando que el IMI es utilizado por múltiples autoridades competentes, en particular muchos departamentos de gobiernos locales que no disponen de los recursos suficientes, se recomienda encarecidamente que las responsabilidades de notificación se coordinen a escala nacional.

([29]) Aunque la conservación de datos personales plantea en comparación menos riesgos para el derecho a la intimidad, el SEPD considera sin embargo que la conservación de datos personales de los usuarios del IMI durante un período de cinco años una vez que ya no tengan acceso al IMI tampoco ha quedado suficientemente justificado.

([30]) Véase el anexo II, apartado I, punto 1.

([31]) Véase asimismo el apartado 12 sobre las recomendaciones relativas a las auditorías.

2.8.2. *Información proporcionada por la Comisión*

67. El artículo 17, apartado 2, letra a), obliga a la Comisión a proporcionar una cláusula de confidencialidad respecto de sus propias actividades de tratamiento de datos, con arreglo a los artículos 10 y 11 del Reglamento (CE) nº 45/2001. Además, el artículo 17, apartado 2, letra b), exige a la Comisión que proporcione asimismo información sobre «los aspectos relativos a la protección de datos en los procedimientos de cooperación administrativa en el IMI según se dispone en el artículo 12». Por último, el artículo 17, apartado 2, letra c), exige a la Comisión que proporcione información sobre «las excepciones o limitaciones de los derechos de los interesados, según se dispone en el artículo 19.».

68. Al SEPD le complace constatar que estas disposiciones contribuyen a la transparencia del tratamiento de datos dentro del IMI. Tal como se ha señalado en el apartado 2.1 *supra*, en el caso de un sistema informático utilizado en 27 Estados miembros resulta fundamental garantizar la coherencia en relación con el funcionamiento del sistema, las garantías aplicadas en materia de protección de datos y la información proporcionada por los interesados ([32]).

69. Dicho lo anterior, las disposiciones del artículo 17, apartado 2, deben reforzarse más. La Comisión, como operador del sistema, es quien dispone de una posición más privilegiada para adoptar una función proactiva a la hora de proporcionar un primer «nivel» del aviso de protección de datos y otra información relevante a los interesados en su sitio web multilingüe, también «en nombre de» las autoridades competentes, es decir, cubriendo la información exigida con arreglo a los artículos 10 y 11 de la Directiva 95/46/CE. De ese modo, bastaría que los avisos proporcionados por las autoridades competentes de los Estados miembros se limitasen a remitirse al aviso de la Comisión, y que lo completaran únicamente en lo necesario para dar cumplimiento a cualquier información adicional específica exigida por el derecho nacional.

70. Además, el artículo 17, apartado 2, letra b), debe clarificar que la información proporcionada por la Comisión abarcará globalmente todos los ámbitos políticos, todos los tipos de procedimientos de cooperación administrativa y todas las aplicaciones dentro del IMI, así como que incluirá específicamente las categorías de datos que pueden ser tratados. Esto debe incluir la publicación de un conjunto de preguntas utilizadas en la cooperación individual en el sitio web del IMI, como, en la actualidad, se está haciendo ya en la práctica.

2.9. **Derechos de acceso, rectificación y cancelación (artículo 18)**

71. El SEPD desea referirse de nuevo, como se ha señalado en el anterior apartado 2.1, al hecho de que resulta fundamental garantizar la coherencia en relación con la explotación del sistema y las garantías aplicadas en materia de protección de datos. Por este motivo, el SEPD desea especificar asimismo las disposiciones relativas a los derechos de acceso, rectificación y cancelación.

72. El artículo 18 debe especificar qué interesados tendrían que presentar una solicitud de acceso. Esto debería quedar claro en relación con el acceso a los datos en los distintos períodos:

— antes de el archivo del asunto,

— después de archivado el asunto, pero antes de que transcurra el plazo de conservación de dieciocho meses,

— y, por último, durante el período en que los datos están «bloqueados».

73. El Reglamento debe exigir también a las autoridades competentes que cooperen en relación con las solicitudes de acceso en los términos necesarios. La corrección y la anulación deberían llevarse a cabo «tan pronto como sea posible aunque a más tardar en 60 días» en lugar de «en 60 días». También debe hacerse referencia a la posibilidad de articular un módulo de protección de datos y a la posibilidad de incluir soluciones de «protección de la intimidad incorporada en el diseño» para la cooperación entre las autoridades en relación con los derechos de acceso, así como la «capacitación de los interesados», por ejemplo, proporcionándoles un acceso directo a sus datos, cuando sea pertinente y viable.

2.10. **Supervisión (artículo 20)**

74. En los últimos años, se ha desarrollado el modelo de «supervisión coordinada». Este modelo de supervisión, actualmente operativo en Eurodac y en partes del Sistema de Información Aduanero, también ha sido adoptado por el Sistema de Información de Visados (VIS) y el Sistema de Información de Schengen de segunda generación (SIS II).

75. Este modelo se articula a tres niveles:

— el control a escala nacional está garantizado por la autoridad nacional de protección de datos,

— el control a escala europea está garantizado por parte del SEPD,

— la coordinación se garantiza mediante reuniones regulares acordadas por el SEPD, quien actúa como secretario de este mecanismo de coordinación.

76. Este modelo se ha revelado fructífero y eficaz y debería estar previsto en el futuro para otros sistemas de información.

77. El SEPD acoge con satisfacción el hecho de que el artículo 20 de la propuesta establezca de manera específica la supervisión coordinada entre las autoridades nacionales de protección de datos y el SEPD siguiendo, en términos amplios, el modelo establecido en los Reglamentos VIS y SIS II ([33]).

([32]) Este enfoque para garantizar la coherencia debería, por supuesto, tener debidamente en cuenta las divergencias nacionales cuando sea necesario y esté justificado.

([33]) Véase el Reglamento (CE) nº 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (DO L 381 de 28.12.2006, p. 4) y el Reglamento (CE) nº 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS) (DO L 218 de 13.8.2008, p. 60).

78. El SEPD reforzaría las disposiciones en materia de supervisión coordinada en determinados puntos y para ello apoya las disposiciones similares aplicadas, por ejemplo, en el contexto del Sistema de Información de Visados (artículos 41 a 43 del Reglamento VIS), el sistema Schengen II (artículos 44 a 46 del Reglamento SIS II) y las previstas para Eurodac ([34]). En particular, sería útil que el Reglamento:

— en el artículo 20, apartados 1 y 2, estableciera y dividiera de manera más clara las correspondientes tareas de supervisión de las autoridades nacionales de protección de datos y del SEPD ([35]),

— en el artículo 20, apartado 3, especificara que las autoridades nacionales de protección de datos y el SEPD, cada uno dentro del ámbito de aplicación de sus competencias, «cooperarán de manera activa» y «garantizarán la supervisión coordinada del IMI» (en lugar de simplemente hacer referencia a la supervisión coordinada sin mencionar la cooperación activa) ([36]); y

— especificara, de forma más detallada, qué cooperación puede tener cabida, por ejemplo, al exigir que las autoridades nacionales de protección de datos y el SEPD «cada uno dentro del ámbito de sus competencias respectivas, intercambiarán la información pertinente, se asistirán mutuamente en la realización de inspecciones y auditorías, estudiarán las dificultades de interpretación y aplicación del Reglamento IMI, examinarán los problemas que se planteen en el ejercicio del control independiente o en el ejercicio de los derechos de los interesados, elaborarán propuestas armonizadas para hallar soluciones comunes a los problemas y fomentarán el conocimiento de los derechos en materia de protección de datos, en la medida necesaria.» ([37]).

79. Dicho esto, el SEPD es consciente del menor tamaño actual, la diferente naturaleza de los datos tratados, así como de la naturaleza cambiante del IMI, por lo que reconoce que sería recomendable una mayor flexibilidad respecto a la frecuencia de las reuniones y las auditorías. En resumen, el SEPD recomienda que el Reglamento proporcione las normas mínimas necesarias para garantizar la cooperación efectiva aunque sin generar cargas administrativas innecesarias.

80. El artículo 20, apartado 3, de la propuesta no exige reuniones regulares sino que simplemente establece que el SEPD puede «invitar a las autoridades nacionales de control a celebrar (…) en caso necesario.». El SEPD acoge con satisfacción el hecho de que estas disposiciones permiten a las partes afectadas decidir la frecuencia y las modalidades de las reuniones, así como otras cuestiones de procedimiento relativas a su cooperación. Lo anterior puede acordarse mediante normas de procedimiento, a las que ya se ha hecho mención en la propuesta.

81. En relación con las auditorías regulares, también pueden ser más eficaces si se permite a las autoridades de cooperación determinar, en sus normas de procedimiento, el momento y la frecuencia con la que se celebrarán dichas auditorías, lo cual puede depender de una serie de factores y también puede variar en el tiempo. Por lo tanto, el SEPD apoya el enfoque de la Comisión, que permite una mayor flexibilidad en este sentido.

2.11. **Utilización del IMI a escala nacional**

82. El SEPD acoge con satisfacción el hecho de que la propuesta establezca un fundamento jurídico claro para la utilización del IMI a escala nacional y que dicha utilización quede sometida a diversas condiciones, en particular el hecho de que la autoridad nacional de protección de datos deba ser consultada y de que el uso deba ajustarse a lo dispuesto en la legislación nacional.

2.12. **Intercambio de información con terceros países (artículo 22)**

83. El SEPD acoge con satisfacción las exigencias establecidas en el artículo 22, apartado 1, para los intercambios de información, así como el hecho de que el artículo 22, apartado 3, garantice la transparencia de la ampliación mediante la publicación en el Diario Oficial de una lista actualizada de los terceros países que utilizan el IMI (artículo 22, apartado 3).

84. El SEPD recomienda asimismo que la Comisión limite la referencia a las excepciones del artículo 26 de la Directiva 95/46/CE con el fin de incluir únicamente el apartado 2 de dicho artículo. En otras palabras, las autoridades competentes u otros agentes externos de un tercer país que no ofrezcan una protección adecuada no deben tener un acceso directo al IMI salvo si existen las adecuadas cláusulas contractuales en vigor. Estas cláusulas deben ser negociadas a escala europea.

85. El SEPD destaca que otras excepciones, como que «la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento legal» no deben emplearse para justificar las transferencias de datos a terceros países utilizando un acceso directo al IMI ([38]).

2.13. **Responsabilidad (artículo 26)**

86. En línea con el refuerzo previsto de las medidas para una mayor responsabilidad durante la revisión del marco europeo de protección de datos ([39]), el SEPD recomienda que el Reglamento establezca un marco claro para los mecanismos de control interno adecuados que garantice el cumplimiento en materia de protección de datos y aporte pruebas en este sentido, incluyendo al menos los elementos que se señalan a continuación.

([34]) Reglamento (CE) nº 2725/2000 del Consejo, de 11 de diciembre de 2000, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín (DO L 316 de 15.12.2000, p. 1), actualmente en revisión. En este contexto, se consideran disposiciones similares a las del Reglamento VIS y del Reglamento SIS II.

([35]) Véanse, por ejemplo, los artículos 41 y 42 del Reglamento VIS.

([36]) Véase, por ejemplo, el artículo 43, apartado 1, del Reglamento VIS.

([37]) Véase, por ejemplo, el artículo 43, apartado 2, del Reglamento VIS.

([38]) Un enfoque similar se ha seguido en el artículo 22, apartado 2, respecto de la Comisión como agente del IMI.

([39]) Véase el apartado 2.2.4. de la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — «Un enfoque global de la protección de los datos personales en la Unión Europea», COM(2010) 609 final. Véase asimismo el apartado 7 del dictamen del SEPD emitido sobre dicha Comunicación de la Comisión el 14 de enero de 2011.

87. En este contexto, el SEPD acoge con satisfacción el requisito del artículo 26, apartado 2, del Reglamento en el que se indica que la Comisión informará, cada tres años, al Supervisor Europeo de Protección de Datos sobre aspectos relativos a la protección de los datos personales, incluida la seguridad de los datos. Sería recomendable que el Reglamento aclarase que, a su vez, podrá exigírsele al SEPD compartir el informe de la Comisión con las autoridades nacionales competentes en materia de protección de datos, en el marco de la supervisión coordinada a la que se hace referencia en el artículo 20. También sería útil aclarar que el informe podrá tratar, por lo que se refiere a cada ámbito político y cada funcionalidad, cómo han sido tratados en la práctica los principios e inquietudes suscitadas por la protección de datos (por ejemplo, la información a los interesados, los derechos de acceso, la seguridad).

88. Además, el Reglamento debe aclarar que el marco de los mecanismos de control interno también debe incluir evaluaciones sobre la protección de la intimidad (incluyendo asimismo un análisis sobre el riesgo para la seguridad), una política de protección de datos (incluido un plan de seguridad) adoptada en función de los resultados de las mismas, así como revisiones y auditorías periódicas.

2.14. **Protección de la intimidad incorporada en el diseño**

89. El SEPD acoge con satisfacción la referencia a este principio incluida en el considerando 6 del Reglamento ([40]). Recomienda que más allá de esta referencia, el Reglamento introduzca igualmente garantías específicas sobre protección de la intimidad incorporada en el diseño, como:

— un módulo de protección de datos que permita a los interesados ejercer más eficazmente sus derechos ([41]),

— un claro aislamiento de los distintos ámbitos políticos incluidos en el IMI («muros protectores») ([42]),

— soluciones técnicas específicas que limiten las capacidades de búsqueda en los directorios, la información de alerta y que, por otras vías, garanticen la limitación a una finalidad específica,

— medidas específicas que garanticen el archivo de los asuntos no activos ([43]),

— garantías de procedimiento adecuadas en el contexto de futuros desarrollos ([44]).

3. **CONCLUSIONES**

90. El dictamen del SEPD sobre el IMI es en general positivo. El SEPD respalda los objetivos de la Comisión de instaurar un sistema electrónico de intercambio de información y de regular aquellos aspectos del sistema relacionados con la protección de datos. El SEPD acoge asimismo con satisfacción el hecho de que la Comisión proponga un instrumento jurídico horizontal para el IMI en forma de Reglamento del Parlamento Europeo y del Consejo. Al SEPD le complace que la propuesta haga especial hincapié en las cuestiones generales relativas a la protección de datos más relevantes para el IMI.

91. Por lo que se refiere al marco jurídico para el IMI que debe establecerse en el Reglamento propuesto, el SEPD llama la atención sobre dos retos principales:

— la necesidad de garantizar la coherencia, al tiempo que se respeta la diversidad, y

— la necesidad de equilibrio entre la flexibilidad y la seguridad jurídica.

92. Las aplicaciones del IMI ya previsibles deben clarificarse y abordarse de manera más específica.

93. Deben aplicarse las adecuadas garantías de procedimiento que aseguren que la protección de datos será cuidadosamente analizada en el contexto de las futuras evoluciones del IMI. Lo anterior debe incluir una evaluación de impacto y una consulta al SEPD y a las autoridades nacionales de protección de datos antes de cada ampliación del ámbito de aplicación del IMI a un nuevo ámbito político o a nuevas aplicaciones.

94. Los derechos de acceso por parte de los agentes externos y el derecho de acceso a las alertas también deben especificarse más detalladamente.

95. En relación con los períodos de conservación:

— el Reglamento debe instaurar garantías de que los casos se archivarán de manera oportuna en el IMI y de que los asuntos inactivos (casos sin ninguna actividad reciente) serán eliminados de la base de datos,

— debe analizarse si existe una justificación adecuada para ampliar el actual período de seis meses a dieciocho meses una vez archivado el asunto,

— la Comisión no ha proporcionado una justificación suficiente de la necesidad y la proporcionalidad de la conservación de los «datos bloqueados» hasta un período de cinco años, por lo que dicha propuesta debe ser reconsiderada,

— debe realizarse una distinción más clara entre las alertas y los registros de información: el Reglamento debe estipular, como norma por defecto que i) —salvo especificación en contrario en la normativa vertical y con sujeción a las adecuadas garantías adicionales— se aplicará un período de conservación de seis meses a las alertas y que ii) dicho período se contabilizará a partir del momento en que se envía la alerta.

96. El Reglamento debe exigir una evaluación del riesgo y una revisión del plan de seguridad antes de cada ampliación del IMI a un nuevo ámbito político o antes de añadir una nueva aplicación que tenga repercusiones sobre los datos personales.

97. Deben reforzarse las disposiciones sobre la información a los interesados y los derechos de acceso y debe fomentarse la adopción de un enfoque más coherente.

([40]) *Ídem*.
([41]) Véase el apartado 2.9. *supra*.
([42]) Véase el apartado 2.4. *supra*.
([43]) Véase el apartado 2.5. *supra*.
([44]) Véase el apartado 2.2.2. *supra*.

98. El SEPD reforzará las disposiciones sobre supervisión coordinada en determinados puntos y para ello apoyaría las disposiciones similares aplicadas, por ejemplo, en el contexto del Sistema de Información de Visados, el sistema Schengen II y las previstas para Eurodac. Por lo que se refiere a la frecuencia de las reuniones y las auditorías, el SEPD apoya el enfoque flexible de la propuesta que tiene por fin garantizar que en el Reglamento se establezcan las normas mínimas necesarias para garantizar la cooperación eficaz sin crear cargas administrativas innecesarias.

99. El Reglamento debe garantizar que las autoridades competentes u otros agentes externos de un tercer país que no ofrezcan una protección adecuada, no cuenten con acceso directo al IMI salvo que estén en vigor las adecuadas cláusulas contractuales. Estas cláusulas deben negociarse a escala europea.

100. El Reglamento debe instaurar un marco claro para los mecanismos de control interno que garantice una efectiva protección de datos y aporte pruebas en este sentido, en particular, las evaluaciones relativas a la protección del derecho a la intimidad (en particular y asimismo un análisis del riesgo para la seguridad), una política de protección de datos (incluido un plan de seguridad) que se adoptará basándose en los resultados de las mismas, así como revisiones y auditorías periódicas.

101. El Reglamento también debe introducir garantías específicas sobre la protección de la intimidad incorporada en el diseño.

Hecho en Bruselas, el 22 de noviembre de 2011.

Giovanni BUTTARELLI

Asistente del Supervisor Europeo de Protección de Datos