I

(Resoluciones, recomendaciones y dictámenes)

DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos sobre 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»

(2011/C 181/01)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su 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], y en particular su artículo 41,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

A. **PARTE GENERAL**

1. **Introducción**

1.1. *Una primera valoración general*

1. El 4 de noviembre de 2010, la Comisión adoptó la Comunicación «Un enfoque global de la protección de los datos personales en la Unión Europea» (en lo sucesivo, la «Comunicación») [3] que se trasladó a efectos de consulta al SEPD. Al SEPD le complace recibir la consulta de la Comisión conforme a lo dispuesto en el artículo 41 del Reglamento (CE) nº 45/2001. Incluso antes de adoptarse la comunicación, el SEPD tuvo ocasión de pronunciarse sobre la Comunicación a título informal. Varias de dichas observaciones han sido recogidas en la versión final del documento.

2. La Comunicación tiene por objeto definir un marco que permita a la Comisión revisar el régimen jurídico de la UE en materia de protección de los datos personales en todos los ámbitos de actuación de la Unión, teniendo en cuenta, en particular, los retos que plantean la globalización y las nuevas tecnologías [4].

3. El SEPD acoge con agrado el texto de la Comunicación en general, puesto que no duda de la necesidad de revisar el presente marco jurídico en materia de protección de datos, con el fin de garantizar la tutela efectiva de los derechos en una sociedad de la información cada vez más compleja. En su dictamen de 25 de julio de 2007 relativo a la aplicación de la Directiva sobre protección de datos [5] el SEPD llegaba ya a la conclusión de que, a largo plazo, sería inevitable introducir modificaciones en la Directiva 95/46/CE.

4. La Comunicación supone un paso importante hacia una modificación normativa que, a su vez, constituirá la evolución más importante en el ámbito de la protección de datos en la UE desde la adopción de la Directiva 95/46/CE, considerada habitualmente la piedra angular de la protección de datos en la Unión Europea (y a mayor escala, en el Espacio Económico Europeo).

5. La Comunicación brinda el marco adecuado para una revisión específica a la vez que arroja luz, en términos generales, sobre los principales problemas y dificultades. El SEPD comparte la opinión de la Comisión en el sentido de que en el futuro seguirá imponiéndose la necesidad de mantener un régimen de protección de datos basado en los principios generales en vigor que regulan la protección de datos, los cuales no han perdido su validez dentro de una sociedad sometida a transformaciones radicales debido a los rápidos avances tecnológicos y a la globalización, lo que obliga a una revisión de las disposiciones legislativas en vigor.

[1] DO L 281 de 23.11.1995, p. 31.
[2] DO L 8 de 12.1.2001, p. 1.
[3] COM(2010) 609 final.
[4] Véase la p. 5 de la Comunicación, párrafo primero.
[5] Dictamen del Supervisor Europeo de Protección de Datos de 25 de julio de 2007 sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos, DO C 255 de 27.10.2007, p. 1.

6. La Comunicación señala acertadamente que los retos son enormes. El SEPD se manifiesta absolutamente de acuerdo y subraya que las soluciones propuestas deben ser, en correspondencia, ambiciosas y contribuir a una protección más eficaz.

1.2. *Objetivo del dictamen*

7. El presente dictamen evalúa las soluciones aportadas en la Comunicación a la luz de dos criterios: su ambición y su eficacia. La impresión del SEPD es, en general, positiva y favorable a la Comunicación, si bien considera que en, determinados aspectos, una visión más ambiciosa hubiera redundado en una mayor eficacia del sistema.

8. El SEPD desea contribuir mediante este dictamen a concretar mejor el marco jurídico en materia de protección de datos. A su vez, aguarda con interés la propuesta de la Comisión prevista para mediados de 2011 y confía en que el texto de la propuesta recoja sus sugerencias. Destaca igualmente que la Comunicación parece omitir determinados ámbitos del instrumento general, caso por ejemplo del tratamiento de datos por parte de las instituciones y los organismos europeos. En caso de que la Comisión realmente decida excluir determinados ámbitos en la presente fase — lo que el SEPD lamentaría — se emplaza a la Comisión a implantar una arquitectura global en un plazo breve y concreto.

1.3. *Elementos esenciales del presente dictamen*

9. El presente dictamen no constituye una manifestación aislada, sino que se inscribe en el contexto de posturas adoptadas anteriormente por el SEPD y por las autoridades europeas responsables de la protección de datos. En especial, debe subrayarse que en el ya mencionado dictamen del SEPD de 25 de julio de 2007, se establecieron y desarrollaron varios elementos a considerar en el marco de futuras modificaciones del marco legal actual ([6]). Asimismo, también se basa en las conversaciones mantenidas con otras partes involucradas en el ámbito de la intimidad y la protección de datos. Sus aportaciones supusieron una referencia muy válida tanto para la Comunicación como para el presente dictamen. A este respecto, puede concluirse que existe un elevado grado de sinergia respecto a cómo mejorar la eficacia de la protección de datos.

10. Otro elemento importante del presente dictamen es el documento denominado «El futuro de la protección de la intimidad», contribución conjunta del Grupo de Trabajo sobre protección de datos del artículo 29, así como del Grupo de Trabajo sobre Policía y Justicia, a la consulta planteada por la Comisión en 2009 (en lo sucesivo, el «documento del Grupo de Trabajo sobre el futuro de la protección de la intimidad») ([7]).

11. Más recientemente, en la Conferencia de prensa de 15 de noviembre de 2010, el SEPD dio a conocer su primera valoración respecto a la presente Comunicación. El presente dictamen se basa en las opiniones de índole más general presentadas durante dicha conferencia de prensa ([8]).

12. Por último, el presente dictamen aprovecha una serie de dictámenes anteriores del SEPD, así como de los documentos del Grupo de Trabajo sobre protección de datos del artículo 29. En diversos lugares del presente dictamen podrán encontrarse, cuando proceda, referencias a dichos dictámenes y documentos.

2. **Contexto**

13. La revisión de las normas que regulan la protección de datos se produce en un momento histórico crucial. La Comunicación describe el contexto exhaustiva y convincentemente. Sobre la base de dicha descripción, el SEPD identifica los cuatro ejes principales que definen el entorno en que se entabla el proceso de revisión.

14. El primer eje es el progreso tecnológico. La tecnología actual ya no es la que existía cuando se concibió y se adoptó la Directiva 95/46/CE. Evoluciones tecnológicas como la computación en nube, la publicidad basada en el comportamiento, las redes sociales, el cobro de peajes en carreteras o los instrumentos de localización geográfica han modificado sustancialmente los métodos utilizados para el tratamiento de datos, y suscitan grandes interrogantes que deberán tenerse en cuenta a la hora de revisar la normativa europea en materia de protección de datos.

15. El segundo eje es la globalización. La progresiva supresión de los obstáculos al comercio ha conferido a las empresas una dimensión crecientemente global. El tratamiento transfronterizo y el trasvase internacional de datos se han incrementado considerablemente en los últimos años. Asimismo, las tecnologías de la información y de la comunicación contribuyen a que el tratamiento de datos sea una realidad en todos los órdenes. Internet y la computación en nube han facilitado el tratamiento deslocalizado de ingentes masas de información a escala mundial. Durante la última década también se han incrementado las actividades policiales y judiciales a escala internacional en el ámbito de la lucha contra el terrorismo y otras formas de delincuencia organizada internacional, basadas en un gran intercambio de información con fines represivos. Todo ello obliga a plantearse seriamente cómo garantizar

([6]) En particular (véase el punto 77 del dictamen): no es necesario modificar los principios existentes, aunque existe una necesidad clara de otros acuerdos administrativos; el amplio alcance de la legislación sobre protección de datos aplicable a cualquier uso de datos personales no debería modificarse; la legislación sobre protección de datos debe permitir un planteamiento equilibrado en casos concretos y permitir también que las autoridades encargadas de la protección de datos fijen prioridades; el sistema debería aplicarse plenamente a la utilización de datos personales a efectos de tratamiento policial, aunque pueden ser precisas medidas adicionales para tratar problemas específicos en este ámbito.

([7]) Documento WP 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). El concepto principal es que las modificaciones legislativas son una buena ocasión para aclarar algunas reglas y principios (como, por ejemplo, el consentimiento y la transparencia), introducir algunos principios nuevos (p. ej., intimidad mediante el diseño, responsabilidad), reforzar la eficacia a través de la modernización de las disposiciones (p. ej., limitando los requisitos de notificación existentes) e incluirlas en un marco jurídico global (incluidas la cooperación policial y judicial).

([8]) Los puntos de la intervención (Speaking Points) de la conferencia de prensa están disponibles en el sitio web del SEPD, en la siguiente dirección: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf

la protección de los datos personales en un mundo globalizado, sin incidir sustancialmente en las operaciones de tratamiento a escala internacional.

16. El tercer eje lo constituye el Tratado de Lisboa. La entrada en vigor del Tratado de Lisboa marca el inicio de una nueva época en materia de protección de datos. El artículo 16 del TFUE no solo recoge el derecho individual del interesado sino que también incorpora un fundamento jurídico directo para una legislación más coherente en materia de protección de datos a nivel europeo. Además, la supresión de la estructura de pilares obliga al Parlamento Europeo y al Consejo a velar por la protección de datos en todos los ámbitos de la legislación europea. En otras palabras, otorga carta de naturaleza a un marco jurídico global en materia de protección de datos aplicable al sector privado y al sector público tanto en el seno de los Estados miembros, así como en el de las instituciones y los organismos europeos. A este respecto, el Programa de Estocolmo ([9]) declara explícitamente que la Unión debe asegurar una estrategia global de protección de datos dentro de la Unión y en sus relaciones con otros países.

17. El cuarto eje es el representado por las evoluciones que están experimentando, en paralelo, las organizaciones internacionales. La modernización de los instrumentos jurídicos vigentes en materia de protección de datos acapara actualmente los debates. En este sentido, es importante recordar las reflexiones que acompañan a la futura revisión del Convenio nº 108 del Consejo de Europa ([10]), así como las Directrices de la OCDE en materia de protección de la intimidad ([11]). Otra evolución importante tiene que ver con la adopción de normas internacionales en materia de protección de datos personales y de la intimidad, que podría materializarse en la adopción de un instrumento jurídico vinculante en materia de protección de datos a escala global. Todas estas iniciativas merecen un apoyo incondicional. Su objetivo común consistirá en garantizar una protección eficaz y uniforme dentro de un entorno globalizado que evoluciona al compás de la tecnología.

3. **Principales perspectivas**

3.1. *La protección de datos fomenta la confianza y debe servir de apoyo a otros intereses (públicos)*

18. Un marco sólido en materia de protección de datos es la consecuencia inevitable de la importancia atribuida a la protección de datos en virtud del Tratado de Lisboa, del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y del artículo 16 del TFUE, y guarda asimismo un estrecho vínculo con las disposiciones del artículo 7 de la Carta ([12]).

19. Sin embargo, un marco sólido en materia de protección de datos también sirve a intereses públicos y privados más amplios en una sociedad de la información donde el tratamiento de datos se ha vuelto omnipresente. La protección de datos promueve la confianza y la confianza constituye a su vez un aspecto esencial del buen funcionamiento de una sociedad. Es esencial imprimir a las disposiciones en materia de protección de datos un sentido que, en la medida de lo posible, suponga un apoyo activo y no un obstáculo para otros derechos e intereses legítimos.

20. Entre dichos intereses legítimos básicos cabe reseñar, entre otros, la solidez de la economía europea, la seguridad de las personas y la transparencia de las políticas gubernamentales.

21. En la Unión Europea, el desarrollo económico discurre en paralelo a la introducción y la comercialización de nuevas tecnologías y nuevos servicios. En la sociedad de la información, el desarrollo y el despliegue adecuados de los servicios y las tecnologías de la información y la comunicación dependen de la confianza. Si los seres humanos no confían en las TIC, el futuro de dichas tecnologías estará fuertemente amenazado ([13]) y los ciudadanos no delegarán en ellas su confianza mientras no perciban que sus datos se encuentran adecuadamente protegidos. Por lo tanto, la protección de datos debe estar implícitamente garantizada para todas las tecnologías y todos los servicios. Un marco sólido en materia de protección de datos proporcionará impulso a la economía europea, a condición de que no solo sea un marco sólido sino que esté también adecuadamente adaptado. Desde este punto de vista, es esencial una mayor armonización dentro de la Unión Europea, así como una minimización de las cargas administrativas (véase el capítulo 5 del dictamen).

22. La necesidad de encontrar un equilibrio entre la seguridad y la protección de la intimidad ha generado acalorados debates durante los últimos años, en particular en relación con los instrumentos para el tratamiento y el intercambio de datos en el ámbito de la cooperación policial y judicial ([14]). Con frecuencia, se ha percibido erróneamente la protección de datos como un obstáculo para la protección total de la seguridad física de las personas ([15]), o, al menos, como una condición que los cuerpos de seguridad deben respetar sine qua non. No debe perderse de vista que un marco sólido en materia de protección de datos puede contribuir a reforzar y fortalecer la seguridad. Los principios que regulan la protección de datos, (de aplicarse correctamente) obligan a los controladores a garantizar que la información es exacta y actualizada y a suprimir de los sistemas los datos personales superfluos e innecesarios para fines policiales. La aplicación de medidas tecnológicas y organizativas que garanticen la seguridad de los sistemas constituye otra posibilidad importante, por

([9]) Programa de Estocolmo — Una Europa abierta y segura que sirva y proteja al ciudadano, DO C 115 de 4.5.2010, p. 1, en el p. 10.

([10]) Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos, DO 108 de 28 de enero de 1981.

([11]) Directrices de la OCDE relativas a la protección de la privacidad y flujos transfronterizos de datos personales, publicadas en http://www.oecd.org

([12]) La importancia de la protección de datos y de su vínculo con la intimidad en la Carta ha sido subrayada por el Tribunal de Justicia en su sentencia de 9 de noviembre de 2010, asuntos acumulados C-92/09 y C-93/09, *Schecke*, todavía no publicada en la Recopilación.

([13]) Véase el Dictamen del SEPD de 18 de marzo de 2010 acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad, DO C 280 de 16.10.2010, p. 1, punto 113.

([14]) Véase por ejemplo el Dictamen de 10 de julio de 2009 sobre la comunicación de la Comisión al Parlamento Europeo y al Consejo relativa a un espacio de libertad, seguridad y justicia al servicios de los ciudadanos, DO C 276 de 17.9.2009, p. 8.

([15]) La seguridad es un concepto más amplio que el de seguridad física pero aquí, al utilizarse como ejemplo de los argumentos debatidos, este concepto cobra una acepción más limitada.

ejemplo, mediante la introducción de sistemas de protección contra la difusión o el acceso no autorizados, como es el caso en el ámbito de la protección de datos.

23. El respeto de los principios que regulan la protección de datos contribuye a garantizar que las autoridades policiales operen conforme al principio del Estado de Derecho, atrayendo así la confianza de la ciudadanía y fomentando, por extensión, la confianza como principio que articula nuestras sociedades. La jurisprudencia establecida en virtud del artículo 8 del Convenio Europeo de Derechos Humanos habilita a las autoridades judiciales y policiales para tratar todos los datos que cooperen de manera eficiente al ejercicio de sus funciones, pero no sin limitaciones. La protección de datos obliga a instaurar salvaguardias (véase el capítulo 9 del dictamen relativo a la policía y la justicia).

24. En las sociedades democráticas, los gobiernos deben rendir cuenta de todos sus actos, en particular la utilización de datos personales en aras a los diversos intereses públicos. Tales actuaciones varían, y pueden ir desde la publicación de datos en Internet por motivos de transparencia, hasta la utilización de datos en apoyo de las políticas en ámbitos como la sanidad pública, el transporte o la fiscalidad, pasando por la vigilancia de las personas con fines represivos. Un marco sólido de protección de datos permite a los gobiernos respetar y asumir sus responsabilidades y responder de sus actos, con arreglo al principio de buena gobernanza.

3.2. *Consecuencias para el marco jurídico en materia de protección de datos*

3.2.1. Necesidad de una mayor armonización

25. La Comunicación subraya justificadamente que una de las deficiencias esenciales del marco actual reside en el hecho de que deja un margen considerable de apreciación a los Estados miembros en lo que se refiere a la transposición de las disposiciones europeas a la legislación nacional. La falta de armonización repercute negativamente a diferentes niveles sobre una sociedad de la información en la que la razón de ser de las fronteras físicas entre los Estados miembros se desdibuja cada vez más (véase el capítulo 5 del dictamen).

3.2.2. Los principios generales que regulan la protección de datos siguen siendo válidos

26. Una primera razón, de índole más formal, por la que los principios generales que regulan la protección de datos no deben ni pueden modificarse es de índole jurídica. Estos principios se recogen en el Convenio nº 108 del Consejo de Europa, vinculante para todos los Estados miembros. Dicho Convenio constituye la base en materia de protección de datos en la Unión Europea. Asimismo, varios de los principios fundamentales se mencionan explícitamente en el artículo 8 de la Carta de Derechos Fundamentales de la Unión. En consecuencia, la modificación de estos principios implicaría la modificación de los Tratados.

27. Pero no es sino una razón y no la única. Otras razones no menos importantes aconsejan no modificar los principios generales. El SEPD está firmemente convencido de que la sociedad de la información ni puede ni debe articularse sin una adecuada protección de la intimidad y de los datos personales de las personas. A mayor cantidad de información procesada, mayor necesidad de protección. Y dentro de una sociedad de la información en la que se procesan ingentes volúmenes de información personal, es necesario que la noción de control por parte de las personas interesadas constituya uno de los fundamentos, facilitando a los ciudadanos actuar como tales y servirse de sus libertades, en particular la libertad de expresión.

28. Además, no es fácil desligar el control ejercido por las personas interesadas de la obligación para los responsables de limitar el tratamiento conforme a los principios de necesidad, proporcionalidad y limitación de los fines. Tampoco es fácil entrever cómo podrían ejercer las personas interesadas su derecho si no se les reconocen derechos tales como el derecho de acceso, de rectificación, de supresión o de bloqueo de los datos.

3.2.3. Perspectiva desde el punto de vista de los derechos fundamentales

29. El SEPD subraya que el derecho a la protección de datos está reconocido como un derecho fundamental, lo cual no significa, no obstante, que la protección de datos deba *prevalecer* siempre por encima de otros derechos e intereses importantes dentro de una sociedad democrática, si bien sus consecuencias se extienden a la naturaleza y el ámbito de aplicación de la protección que un marco jurídico europeo debe proporcionar, a fin de garantizar, de este modo, que se tengan *pertinentemente* en cuenta las obligaciones en materia de protección de datos.

30. Estas consecuencias principales pueden definirse en los siguientes términos:

— la protección debe ser efectiva. El marco jurídico debe proporcionar instrumentos que permitan a los particulares ejercer sus derechos en la práctica;

— el marco debe permanecer estable a largo plazo;

— la protección debe garantizarse en todas las circunstancias y no depender de las preferencias políticas en un período determinado;

— es necesario fijar limitaciones al ejercicio del derecho, si bien dichas limitaciones deben ser excepcionales, estar debidamente justificadas y en ningún caso afectar a los elementos esenciales del propio derecho ([16]).

El SEPD recomienda que la Comisión tome en consideración estas consecuencias en el momento de proponer soluciones legislativas.

3.2.4. Necesidad de nuevas disposiciones legislativas

31. La Comunicación se centra acertadamente en la necesidad de reforzar las disposiciones legislativas en materia de protección de datos. En este contexto, cabe recordar que en el documento del Grupo de Trabajo sobre el futuro de la protección de la intimidad ([17]) las autoridades

([16]) Véase asimismo el Dictamen del Supervisor Europeo de Protección de Datos de 25 de julio de 2007 sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos, p. 17, que se basa en la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia.

([17]) Véase la nota a pie de página 7.

responsables de protección de datos pusieron especial acento en la necesidad de reforzar el papel de los diferentes actores en el ámbito de la protección de datos, en especial los interesados, los responsables del tratamiento de los datos y las propias autoridades encargadas de la vigilancia.

32. Todas las partes involucradas coinciden en que unas disposiciones legislativas más sólidas, en las que se tengan en cuenta los progresos tecnológicos y la globalización, son la clave para una protección de datos ambiciosa y eficaz en el futuro. Como se indica en el apartado 7, tales son los criterios que el SEPD debe evaluar para cada una de las soluciones propuestas.

3.2.5. La exhaustividad como condición sine qua non

33. Como se recuerda en la Comunicación, la Directiva 95/46/CE es aplicable a todas las actividades de tratamiento de datos personales en los Estados miembros, tanto en el sector público como en el privado, con excepción de las actividades no incluidas en el ámbito de aplicación del anterior Derecho comunitario ([18]). Aunque esta excepción era necesaria en virtud del Tratado anterior, la situación ha variado tras la entrada en vigor del Tratado de Lisboa. A la vez, la excepción es contraria tanto a la redacción como al espíritu del artículo 16 del TFUE.

34. En opinión del SEPD, la introducción de un instrumento jurídico global en materia de protección de datos, que incluyese la cooperación policial y judicial en materia penal, debe considerarse una de las posibles mejoras derivadas de un nuevo marco jurídico. Resulta, pues, una condición *sine qua non* para que la protección de datos sea eficaz en el futuro.

35. El SEPD avanza los siguientes argumentos en apoyo de esta afirmación:

— la distinción entre operaciones del sector privado y operaciones de las fuerzas de seguridad se desdibuja cada vez más. Las entidades del sector privado tratan datos que se utilizarán en último término a efectos de de ejecución de la ley (por ejemplo, los datos PNR ([19])), mientras que en otros casos se les obliga a conservar los datos para los mismos fines s (por ejemplo, la Directiva sobre conservación de datos ([20]));

— no existe diferencia fundamental entre las autoridades policiales y judiciales y el resto de autoridades encargadas del cumplimiento de la ley (fiscalidad, aduanas, lucha contra el fraude, inmigración), con arreglo a la Directiva 95/46/CE;

— como bien se afirma en la Comunicación, el instrumento jurídico de protección de datos actualmente aplicable a las autoridades policiales y judiciales [Decisión marco 2008/977/JAI ([21])] es inadecuado;

— la mayoría de los Estados miembros han transpuesto la Directiva 95/46/CE y el Convenio nº 108 en sus respectivas legislaciones nacionales, haciéndolas así aplicables igualmente para las autoridades policiales y judiciales.

36. La inclusión del ámbito policial y judicial en el instrumento jurídico general no solo brindaría más garantías a los ciudadanos sino que también facilitaría el trabajo de las autoridades policiales. Aplicar conjuntos de normas diferenciados es gravoso, supone una innecesaria pérdida de tiempo a la vez que un freno para la cooperación internacional (véase el capítulo 9 del presente dictamen), lo que también es motivo para incluir las actividades de tratamiento por parte de los servicios de seguridad nacionales, en la medida de lo posible, en el marco de la legislación europea en vigor.

3.2.6. La neutralidad tecnológica

37. El período que siguió a la adopción de la Directiva 95/46/CE en 1995 puede calificarse, desde el punto de vista tecnológico, como un periodo agitado, marcado por la aparición sucesiva y frecuente de nuevas tecnologías y aplicaciones tecnológicas que, en muchos casos, provocaron cambios esenciales de los procedimientos utilizados para el tratamiento de los datos personales. La sociedad de la información ya no es un entorno paralelo al que los ciudadanos tienen la oportunidad de acceder si así lo desean, sino que se ha convertido, por el contrario, en un elemento más de nuestra vida cotidiana. Por ejemplo, la noción de Internet de los objetos ([22]) establece vínculos entre los objetos físicos y la información en línea con ellos relacionada.

38. La tecnología seguirá evolucionando, lo que repercutirá en el nuevo marco jurídico. La tecnología deberá mantenerse eficiente durante períodos más prolongados, sin lastrar a su vez eventuales avances tecnológicos, lo que obligará a adoptar disposiciones neutras desde el punto de vista jurídico. No obstante, el marco también debe aportar mayor seguridad jurídica a las empresas y los particulares, que deberán entender qué se espera de ellos y habrán de estar capacitados para hacer valer sus derechos, por lo que las disposiciones jurídicas deberán ser precisas.

39. En opinión del SEPD, el instrumento jurídico general en materia de protección de datos deberá formularse, dentro de lo posible, en términos tecnológicamente neutros, lo que implica que los derechos y obligaciones de los diferentes actores deberán señalarse en términos neutros y generales de manera que sigan siendo, en principio, válidos y aplicables independientemente de la tecnología

([18]) El presente dictamen se centrará principalmente en el anterior tercer pilar (cooperación policial y judicial en materia penal), ya que el anterior segundo pilar no solo es un ámbito más complicado de la legislación comunitaria (como también se reconoce en el artículo 16 del TFUE y en el artículo 39 del TUE), sino que posee una relevancia menor en relación con el tratamiento de datos.

([19]) Véase, por ejemplo, la Comunicación de la Comisión sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países, COM(2010) 492 final.

([20]) Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios en comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO L 105 de 13.4.2006, p. 54).

([21]) Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO L 350 de 30.12.2008, p. 60).

([22]) Tal como se define en el documento «Internet de los objetos — Un plan de acción para Europa», COM(2009) 278 final.

elegida para el tratamiento de los datos personales. No hay otra opción, habida cuenta de la rápida evolución de los avances tecnológicos en la actualidad. El SEPD sugiere introducir nuevos derechos «neutros desde el punto de vista tecnológico» además de los principios existentes en materia de protección de datos, lo cual podría ser especialmente relevante en un entorno electrónico que evoluciona rápidamente (véanse en particular los capítulos 6 y 7).

3.2.7. Largo plazo: seguridad jurídica a más largo plazo

40. La Directiva 95/46/CE ha sido el elemento clave en materia de protección de datos en la Unión Europea durante los últimos quince años. Esta Directiva fue incluida en la legislación de los Estados miembros y aplicada por los distintos agentes. A lo largo de los años, dicha aplicación se ha enriquecido con las diversas experiencias prácticas y las nuevas orientaciones proporcionadas por la Comisión, las autoridades encargadas de protección de datos (tanto a nivel nacional como en el marco del Grupo de Trabajo del «artículo 29») así como por los tribunales nacionales y europeos.

41. Conviene indicar que estas evoluciones precisan tiempo y que, por tratarse especialmente de un marco general que da efecto a un derecho fundamental, ese tiempo es fundamental para crear seguridad y estabilidad jurídicas. Debe elaborarse un nuevo instrumento jurídico general con el fin de garantizar la seguridad y estabilidad jurídicas durante un período más prolongado, y teniendo en cuenta que es muy difícil aventurar el curso que seguirán la tecnología y la globalización. En cualquier caso, el SEPD apoya sin reservas el objetivo de crear seguridad jurídica durante un período más prolongado, comparable a la perspectiva de la Directiva 95/46/CE. En resumen, cuando la tecnología evoluciona a un ritmo rápido, la legislación debe mantenerse estable.

3.2.8. Corto plazo: hacer mejor uso de los instrumentos existentes

42. A corto plazo, es fundamental garantizar la eficacia de las disposiciones legislativas existentes, concentrándose en primer lugar en su aplicación, tanto a nivel nacional como a nivel de la UE (véase el capítulo 11 del presente dictamen).

B. **ELEMENTOS DE UN NUEVO MARCO**

4. **Enfoque global**

43. El SEPD apoya plenamente el enfoque global en materia de protección de datos, que no sólo es el enunciado sino también el punto de partida de la Comunicación e incluye necesariamente la ampliación de las normas generales en materia de protección de datos a la cooperación policial y judicial en materia penal ([23]).

44. No obstante, observa también que la Comisión no pretende incluir todas las actividades de tratamiento de datos en este instrumento jurídico general. En particular, no se incluirá el tratamiento de datos por parte de las instituciones, órganos, oficinas y agencias de la Unión Europea. La Comisión se limita a declarar que «evaluará la necesidad de adaptar otros instrumentos jurídicos al nuevo marco general de la protección de datos».

45. El SEPD se inclina decididamente por la inclusión del tratamiento a nivel europeo en el marco jurídico general. Recuerda que ésta fue la intención original del antiguo artículo 286 del TCE, en el que por primera vez se hizo referencia a la protección de datos a nivel de Tratado. El artículo 286 del TCE afirmaba simplemente que los instrumentos jurídicos en materia del tratamiento de datos personales también se aplicarán a las instituciones. Lo más relevante es que un texto jurídico único permite evitar todo riesgo de discrepancia entre disposiciones y sería particularmente adecuado para el intercambio de datos entre la Unión y las entidades públicas y privadas de los Estados miembros. Permitiría evitar a su vez el riesgo de que, una vez modificada la Directiva 95/46/CE, no existiese interés político alguno en modificar el Reglamento (CE) nº 45/2001 o en conceder a dicha modificación la suficiente prioridad como para evitar discrepancias sobre las fechas de entrada en vigor.

46. El SEPD insta a la Comisión, en caso de que, a su juicio, no fuera factible incluir el tratamiento a nivel de la Unión en el instrumento jurídico general, a que se comprometa a proponer una versión adaptada del Reglamento (CE) nº 45/2001 (no a que «evalúe la necesidad») en el plazo más breve posible y preferentemente antes de finales de 2011.

47. No es menos importante que la Comisión garantice una atención similar en otros ámbitos, en particular:

— la protección de datos en la Política de Exterior y de Seguridad Común, sobre la base del artículo 39 del TUE ([24]);

— los regímenes de protección de datos por sectores específicos para los órganos de la Unión como Europol, Eurojust y para los sistemas de información a gran escala, en la medida en que deban adaptarse al nuevo instrumento jurídico;

— la Directiva 2002/58/CE sobre protección de la intimidad, en la medida en que deba ser adaptada al nuevo instrumento jurídico.

48. Por último, un instrumento jurídico general en materia de protección de datos puede, y probablemente debe, ser completado mediante normativas específicas y sectoriales adicionales, por ejemplo en materia de cooperación policial y judicial, aunque también en otros ámbitos ([25]). En la medida en que sea necesario y con arreglo al principio de subsidiariedad, deberán adoptarse dichas disposiciones adicionales a nivel de la Unión Europea. Los Estados miembros podrán elaborar normas adicionales en ámbitos específicos en los que estas normas estén justificadas (véase el punto 5.2).

([23]) Véase el punto 14 de la Comunicación y el punto 3.2.5 del presente dictamen.

([24]) Véase asimismo el Dictamen del Supervisor Europeo de Protección de Datos de 24 de noviembre de 2010 sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo «La política antiterrorista de la UE: logros principales y retos futuros», punto 31.

([25]) Véase asimismo el documento del Grupo de Trabajo sobre el futuro de la protección de la vida privada (nota a pie de página nº 7), puntos 18-21.

5. **Mayor armonización y simplificación**

5.1. *La necesidad de armonización*

49. La armonización es un elemento crucial para la legislación europea en materia de protección de datos. La Comunicación señala acertadamente que la protección de datos reviste una considerable importancia para el mercado interior, ya que debe garantizar la libre circulación de los datos personales entre los Estados miembros en el mercado interior. Sin embargo, el grado de armonización en virtud de la actual Directiva no se ha considerado suficientemente satisfactorio. La Comunicación reconoce que éste es uno de los motivos de preocupación para las partes involucradas. En particular, las partes involucradas destacan la necesidad de incrementar la seguridad jurídica, reducir las cargas administrativas y garantizar la igualdad de condiciones a los agentes económicos y otros responsables del tratamiento de datos. Como la Comisión observa acertadamente, tal es el caso, en particular, de los responsables del tratamiento de datos establecidos en varios Estados miembros y obligados a cumplir requisitos y prácticas (probablemente distintos) de las legislaciones nacionales sobre protección de datos ([26]).

50. La armonización no solo es importante para el mercado interior sino también para garantizar una adecuada protección de datos. El artículo 16 del TFUE establece que «toda persona» tiene derecho a la protección de los datos de carácter personal que le conciernan. Para que dicho derecho sea efectivamente respetado, debe garantizarse un nivel equivalente de protección en todo el territorio de la Unión Europea. El documento del Grupo de Trabajo sobre la protección de la intimidad en el futuro destaca que varias de las disposiciones relativas a la situación de los titulares de los datos no ha sido aplicada o no ha sido interpretada de manera uniforme en todos los Estados miembros ([27]). En un mundo globalizado e interconectado, estas divergencias pueden amenazar o limitar la protección de los particulares.

51. El SEPD considera que uno de los principales objetivos de la revisión consiste en mantener y mejorar la armonización. El SEPD acoge con agrado el compromiso de la Comisión de examinar los medios para lograr una protección de datos más armonizada a nivel europeo. Sin embargo, le sorprende constatar que la Comunicación no formule en esta fase ninguna opción concreta. Asimismo, indica diversos ámbitos en los que mejorar la convergencia resulta más apremiante (véase la sección 5.3). La mayor armonización en estos ámbitos no solo debe lograrse mediante la reducción del margen de maniobra de la legislación nacional sino también evitando una aplicación incorrecta por parte de los Estados miembros (véase asimismo el capítulo 11) y garantizando una aplicación más coherente y coordinada (véase también el capítulo 10).

([26]) Comunicación, p. 10.

([27]) Véase el Documento del Grupo de Trabajo sobre el futuro de la protección de la vida privada (nota a pie de página nº 7), punto 70. El documento se refiere en particular a las disposiciones de responsabilidad y a la posibilidad de reclamar daños inmateriales.

5.2. *Reducción del margen de maniobra en materia de aplicación de la Directiva*

52. La Directiva incluye una serie de disposiciones formuladas de manera general y que, por lo tanto, dejan un margen de maniobra significativo para que se produzcan diferencias en la aplicación. El considerando 9 de la Directiva confirma de manera explícita que los Estados miembros disponen de un margen de maniobra y que, dentro de los límites de dicho margen, pueden surgir disparidades en la aplicación de la Directiva. Los Estados miembros han aplicado en términos diferentes diversas disposiciones, particularmente varias disposiciones fundamentales ([28]). Esta situación no resulta satisfactoria y es preciso explorar una mayor convergencia.

53. Esto no significa que deba excluirse inmediatamente la diversidad. En determinados ámbitos, puede revelarse necesaria la flexibilidad con el fin de preservar las especificidades que resulten justificadas, proteger los intereses públicos importantes o la autonomía institucional de los Estados miembros. A juicio del SEPD, el margen de divergencia entre los Estados miembros debe limitarse en concreto a las siguientes situaciones específicas:

— Libertad de expresión: en virtud del presente marco (artículo 9), los Estados miembros pueden establecer exenciones y excepciones en lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria. Dicha flexibilidad parece adecuada, siempre que esté sujeta a los límites de la Carta y del CEDH, teniendo en cuenta las distintas tradiciones y diferencias culturales que puedan existir en este ámbito en los Estados miembros. Sin embargo, ello no constituirá un obstáculo para la posible actualización del artículo 9, en vista de los avances de Internet.

— Intereses públicos específicos: en virtud del presente marco (artículo 13), los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos cuando tal limitación constituya una medida necesaria para la salvaguardia de un interés público importante, como la seguridad del Estado, la defensa, la seguridad pública, etc. Esta competencia de los Estados miembros sigue estando justificada. Sin embargo, la interpretación de las excepciones deberá armonizarse más llegado el caso (véase la sección 9.1). Además, el actual ámbito de aplicación de la excepción contemplada en el artículo 6, apartado 1, parece indebidamente amplio.

— Vías de recurso, sanciones y procedimientos administrativos: un marco europeo debe determinar las condiciones principales aunque, en virtud de la situación actual de la legislación de la Unión, la determinación de las sanciones, vías de recurso, normas procesales y las modalidades de controles aplicables a escala nacional debe quedar en manos de los Estados miembros.

([28]) También existen enfoques diferentes respecto de los datos manuales.

5.3. *Ámbitos que requieren una mayor armonización*

54. *Definiciones* (artículo 2 de la Directiva 95/46/CE). Las definiciones son la piedra angular del régimen jurídico y deberán interpretarse de manera uniforme en todos los Estados miembros, sin margen de aplicación. En virtud del presente marco han surgido divergencias, por ejemplo en relación con el concepto de responsable del tratamiento ([29]). El SEPD sugiere añadir más elementos a la lista actual del artículo 2, como los datos anónimos, los seudónimos, los datos judiciales, la transferencia de datos y el responsable de la protección de datos, con el fin de proporcionar una mayor seguridad jurídica.

55. *Licitud del tratamiento (artículo 5).* El nuevo instrumento jurídico deberá ser lo más preciso posible en relación con los elementos esenciales que determinan la licitud del tratamiento de los datos. El artículo 5 de la Directiva (así como el considerando 9), que establece que los Estados miembros precisarán las condiciones en que son lícitos los tratamientos de datos personales, podría dejar de ser necesario en un marco futuro.

56. *Motivos para el tratamiento de datos* (artículos 7 y 8). La definición de las condiciones para el tratamiento de datos constituye un elemento esencial de toda legislación en materia de protección de datos. No se debe permitir a los Estados miembros que introduzcan modificaciones a los motivos o motivos adicionales para el tratamiento o que excluyan alguno de ellos. Debe excluirse o limitarse la posibilidad de establecer excepciones (en especial respecto a los datos sensibles ([30])). En el nuevo instrumento jurídico, deben formularse con toda claridad los motivos para el tratamiento de datos, reduciendo así el margen de apreciación en la aplicación o en el control de la aplicación. En particular, es necesario especificar más claramente el concepto de consentimiento (véase la sección 6.5). Además, el motivo basado en el interés legítimo del responsable del tratamiento de datos [artículo 7, letra f)] permite interpretaciones extremadamente divergentes, debido a su carácter flexible. Es necesaria una mayor armonización. Otra disposición que posiblemente haya de especificarse es el artículo 8, apartado 2, letra b), que permite el tratamiento de datos sensibles cuando sea necesario para respetar las obligaciones y los derechos específicos del responsable del tratamiento en materia de Derecho laboral ([31]).

57. *Derechos de los interesados* (artículos 10-15). Este es uno de los ámbitos en el que no todos los elementos de la Directiva han sido aplicados o interpretados coherentemente por parte de los Estados miembros. Los derechos de los interesados son un elemento central en la protección efectiva de los datos, por lo que el margen de maniobra deberá reducirse sustancialmente. El SEPD recomienda que la información proporcionada a los interesados por el responsable del tratamiento sea uniforme en toda la Unión Europea.

58. *Transferencias internacionales* (artículos 25-26). Este ámbito ha suscitado profundas críticas debido a la falta de una práctica uniforme en toda la Unión. Las partes involucradas han criticado que los Estados miembros interpreten y apliquen de manera muy diferente las decisiones de la Comisión respecto al carácter adecuado. Las normas vinculantes para las empresas son otro elemento en el que el SEPD aboga por una mayor armonización (véase el capítulo 9).

59. *Autoridades nacionales de protección de datos* (artículo 28). Las autoridades nacionales de protección de datos están sujetas a normas sumamente divergentes en los 27 Estados miembros, en especial en lo que se refiere a su estatuto, recursos y competencias. El artículo 28 ha alimentado en parte dichas divergencias debido a su imprecisión ([32]) y debe especificarse más, con arreglo a lo establecido en la Sentencia del Tribunal de Justicia Europeo en el asunto C-518/07 ([33]) (para más información, véase el capítulo 10).

5.4. *Simplificación del sistema de notificación de ficheros*

60. Los requisitos de notificación (artículos 18-21 de la Directiva 95/46/CE) son otro ámbito en el que los Estados miembros disponían hasta la fecha de un significativo margen de libertad. La comunicación reconoce atinadamente que un sistema armonizado permitiría reducir los costes y las cargas administrativas para los responsables del tratamiento de datos ([34]).

61. En este ámbito, la simplificación debería ser el objetivo principal. La revisión del marco de protección de datos brinda una ocasión única para simplificar o reducir más el ámbito de los actuales requisitos de notificación. La Comunicación reconoce que la mayoría de los responsables del tratamiento coinciden en que la obligación general de notificar todas las operaciones de tratamiento a las autoridades encargadas de la protección de datos es relativamente gravosa y no aporta, en sí, un verdadero valor añadido desde el punto de vista de la protección de los datos personales ([35]). Por ello, el SEPD acoge con agrado el compromiso de la Comisión de estudiar los diferentes medios para simplificar el actual sistema de notificación de ficheros.

62. En su opinión, el punto de partida de dicha simplificación contribuiría a un cambio de sistema en el que la notificación es la norma general, salvo que se prevea lo contrario (es decir, el «sistema de exención»), a un sistema más específico. El sistema de exención se ha revelado ineficaz, ya que su aplicación ha sido incoherente en los Estados miembros ([36]). El SEPD sugiere que se consideren las siguientes alternativas:

([29]) Véase el Dictamen 1/2010 del Grupo de Trabajo del artículo 29 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (WP 169).

([30]) El artículo 8, apartados 4 y 5, actualmente autoriza que en determinadas condiciones los Estados miembros establezcan otras excepciones en relación con los datos sensibles.

([31]) Véase a este respecto, el primer informe de la Comisión sobre la aplicación de la Directiva sobre protección de datos mencionado anteriormente, p. 14.

([32]) Documento del Grupo de Trabajo sobre el futuro de la protección de la intimidad, punto 87.

([33]) Asunto C-518/07, *Comisión/Alemania,* todavía no publicado en la Recopilación.

([34]) Véase la nota a pie de página 26.

([35]) Véase la nota a pie de página 26.

([36]) Informe del Grupo de Trabajo del artículo 29 relativo a la obligación de notificación a las autoridades nacionales de control, la mejor utilización de las excepciones y las simplificaciones y el papel de los responsables de protección de datos en la Unión Europea, WP 106, 2005, p. 7.

— limitar la obligación de notificar a los tipos específicos de operaciones de tratamiento que presentan riesgos específicos (estas notificaciones podrían requerir otros pasos, como el control previo del tratamiento);

— establecer una obligación simplificada de registro que obligue a que sean los responsables del tratamiento de datos los que realicen dicho registro (por oposición al registro exhaustivo de todas las operaciones de tratamiento de datos);

Además, podría introducirse un formulario de notificación estándar paneuropeo con el fin de garantizar enfoques armonizados relativos a la información solicitada.

63. La revisión del actual sistema de notificación debe entenderse sin perjuicio de la mejora de las obligaciones de control previo para determinadas obligaciones de tratamiento que puedan presentar riesgos específicos (como los sistemas de información a gran escala). El SEPD sería partidario de la inclusión en el nuevo instrumento jurídico de una lista no exhaustiva de casos para los que se requiere un control previo. El Reglamento (CE) nº 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios proporciona un modelo útil en este sentido ([37]).

5.5. *Un Reglamento, no una Directiva*

64. Por último, el SEPD entiende que el proceso de revisión brinda asimismo una oportunidad para reconsiderar el tipo de instrumento jurídico aplicable en materia de protección de datos. Un reglamento, único instrumento directamente aplicable en los Estados miembros, es el medio más eficaz para proteger el derecho fundamental a la protección de datos y para crear un mercado interior real en el que los datos personales puedan circular libremente y el nivel de protección sea similar, independientemente del país o del sector en el que se efectúe el tratamiento de los datos.

65. Un reglamento reduciría el margen de interpretaciones contradictorias y de divergencias injustificadas en la incorporación y en la aplicación de la ley. También reduciría la importancia de determinar la ley aplicable a las operaciones de tratamiento en la Unión Europea, que es uno de los aspectos más controvertidos del sistema actual (véase el capítulo 9).

66. En el ámbito de la protección de datos, un reglamento se justifica, con mayor razón, por el hecho de que

— el artículo 16 del TFUE eleva al nivel de Tratado el derecho a la protección de los datos personales y prevé — o incluso establece — un nivel uniforme de protección de las personas físicas en toda la Unión,

— el tratamiento de datos tiene lugar en un entorno electrónico en el que las fronteras internas entre los Estados miembros han perdido relevancia.

67. Optar por un reglamento como instrumento general permite, llegado el caso, la existencia de disposiciones directamente dirigidas a los Estados miembros en las que es necesaria una cierta flexibilidad. Asimismo, tampoco influye en la competencia de los Estados miembros para adoptar normas complementarias en materia de protección de datos, en su caso, con arreglo al Derecho de la Unión.

6. **Reforzar los derechos de las personas**

6.1. *La necesidad de reforzar los derechos*

68. El SEPD apoya sin reservas la propuesta de la Comunicación que pasa por reforzar los derechos individuales, ya que los instrumentos jurídicos existentes no garantizan plenamente una protección eficaz necesaria en un mundo digitalizado y cada vez más complejo.

69. Por otro lado, el advenimiento de un universo digitalizado lleva aparejado un claro incremento de la obtención, el uso y posterior transferencia de los datos personales de un modo muy complejo y en absoluto transparente. Por lo general, las personas no saben o no comprenden cómo se desarrolla este proceso, quiénes obtienen sus datos ni de qué medios disponen para controlar la situación. Un hecho que sirve para ilustrar el fenómeno es el control de las actividades de navegación por parte de los proveedores de redes publicitarias, que utilizan «chivatos» (*cookies*) u otros dispositivos similares para proponer unos objetivos publicitarios. Cuando los internautas visitan sitios web, no cuentan con que terceras personas vayan a registrar dichas visitas ni creen registros de los usuarios sobre la base de informaciones que revelen su estilo de vida, o sus gustos.

70. Por otra parte, esta evolución incita a la ciudadanía a compartir voluntariamente sus informaciones personales, por ejemplo en las redes sociales, que atraen a un número cada vez mayor de jóvenes ansiosos de comunicarse con jóvenes de su misma edad. No es muy factible que los jóvenes (internautas) sean conscientes del alcance de la divulgación de dichas informaciones ni de las repercusiones sobre sus actos a largo plazo.

6.2. *Aumentar la transparencia*

71. La transparencia es vital en todo régimen de protección de datos, no solo por su valor intrínseco sino también porque permite ejercer otros principios relacionados con la protección de datos. Los individuos solo podrán ejercer sus derechos si saben de la existencia del tratamiento de datos.

72. Varias disposiciones de la Directiva 95/46/CE guardan relación con la transparencia. Los artículos 10 y 11 contemplan la obligación de informar a los ciudadanos sobre la obtención de los datos personales que les afectan. Además, el artículo 12 reconoce el derecho a recibir una comunicación, en forma inteligible, de los propios datos personales objeto de tratamiento (derecho de acceso). El artículo 15 reconoce el derecho de acceder al mecanismo subyacente a la toma de decisiones automatizadas que tienen efectos jurídicos. Por último, e igualmente importante, el artículo 6, apartado 1, letra a), obliga a que los datos sean tratados de manera leal, y genera igualmente una obligación de transparencia. Los datos personales no pueden tratarse con fines ocultos o secretos.

([37]) Véase el artículo 27 del Reglamento, DO L 8 de 12.1.2001, p. 1.

73. La Comunicación sugiere añadir un principio general de transparencia. Como reacción frente a dicha sugerencia, el SEPD subraya que el concepto de transparencia ya es inherente al marco jurídico vigente en materia de protección de datos, si bien de manera implícita. Así se deduce de las diversas disposiciones relativas a la transparencia, como se ha mencionado en el apartado anterior. Según el SEPD, la inclusión de un principio *explícito* de transparencia podría ser de interés, independientemente de que esté vinculado o no a la disposición ya existente relativa a un tratamiento leal, ya que aumentaría la seguridad jurídica y también confirmaría que un responsable del tratamiento debe, bajo toda circunstancia, tratar los datos personales de modo transparente, no solo cuando se le emplaza a que así lo haga o cuando se lo imponga una disposición jurídica específica.

74. Sin embargo, quizá es más importante reforzar las disposiciones existentes relativas a la transparencia, como los artículos 10 y 11 de la Directiva 95/46/CE. Dichas disposiciones especifican los elementos informativos que habrán de proporcionarse aunque sin precisar las modalidades. En términos más concretos, el SEPD sugiere reforzar las disposiciones existentes mediante la incorporación de:

— un requisito que obligue al encargado del tratamiento a proporcionar información sobre el tratamiento de los datos de manera clara y comprensible, a la vez que en un lenguaje claro y sencillo ([38]). La información debe ser clara, evidente y destacada. Dicho servicio podría englobar igualmente la obligación de garantizar que la información sea fácilmente comprensible. Esta obligación contribuiría a proscribir las políticas de confidencialidad confusas o no fácilmente comprensibles;

— un requisito que obligue a facilitar la información a los interesados de manera sencilla y directa. La información también deberá ser permanente, accesible y no deberá suprimirse de un medio electrónico al cabo de un breve período, lo que ayudaría a los usuarios a conservar y reproducir la información en el futuro, permitiendo el acceso ulteriormente.

6.3. *Apoyo a la obligación de informar sobre las violaciones de la seguridad*

75. El SEPD apoya la introducción en el instrumento general de una disposición relativa a la notificación de las violaciones de los datos personales, que amplía la obligación contemplada en la Directiva sobre la protección de la intimidad en las comunicaciones electrónicas a todos los responsables del tratamiento, tal como se desprende de la Comunicación. En el marco de esta Directiva, modificada en Noviembre 2009, la obligación es aplicable solamente a los proveedores de servicios de comunicaciones electrónicas (proveedores de servicios de telefonía, incluidos los servicios de VoIP, y de acceso a Internet). La obligación no abarca a otros responsables del tratamiento. Sin embargo, los motivos que justifican la obligación son enteramente aplicables a aquellos responsables del tratamiento diferentes de los proveedores de servicios de comunicaciones electrónicas.

76. La notificación de violaciones de la seguridad persigue fines y objetivos diferenciados. El más evidente, resaltado en la Comunicación, es el de servir como herramienta de información para que la ciudadanía cobre conciencia de los riesgos a los que se enfrenta cuando sus datos personales se ven afectados, lo que podría ayudarles a adoptar las medidas necesarias para atenuar los riesgos. Por ejemplo, cuando se les alerta sobre violaciones que afectan a su información económica, las personas podrán, entre otras cosas, modificar sus contraseñas o cancelar sus cuentas. Además, la notificación de una violación de la seguridad contribuye a la aplicación eficaz de otros principios y obligaciones de la Directiva. Por ejemplo, los requisitos de notificación de violaciones de la seguridad animan a los responsables del tratamiento a aplicar medidas de seguridad más estrictas con objeto de evitarlas. La violación de la seguridad también es un instrumento para reforzar la responsabilidad de los responsables del tratamiento y, más en particular, para aumentar la responsabilidad de los mismos (véase el capítulo 7). Por último, sirve como herramienta para la ejecución, por parte de las autoridades encargadas de la protección de datos. La notificación de una violación a dichas autoridades podría iniciar una investigación sobre las prácticas generales de los responsables del tratamiento de datos.

77. Las normas específicas relativas a la violación de la seguridad en la Directiva sobre la protección de la intimidad modificada fueron objeto de amplios debates durante la tramitación parlamentaria del marco jurídico que precedió a la adopción de dicha Directiva. En dicho debate, se tuvieron en cuenta los dictámenes del Grupo de Trabajo del «artículo 29» y del SEPD, junto con las opiniones de las partes involucradas. Las normas reflejan las opiniones de las diferentes partes involucradas y representan un equilibrio de intereses: los criterios que desencadenan la obligación de notificación son, en principio, adecuados para garantizar la protección de las personas, pero no imponen obligaciones inútiles ni excesivamente gravosas.

6.4. *Reforzar el consentimiento*

78. El artículo 7 de la Directiva sobre la protección de datos menciona seis fundamentos jurídicos para el tratamiento de los datos personales. El consentimiento de la persona física es uno de ellos. A los responsables del tratamiento se les permite tratar datos personales en la medida en que las personas hayan prestado su consentimiento informado para la obtención y posterior tratamiento de sus datos.

79. En la práctica, los usuarios no pueden ejercer por lo general sino un control limitado de sus datos, en especial

([38]) Véase la comunicación, p. 6.

en un entorno tecnológico. Uno de los métodos ocasionalmente utilizados es el consentimiento implícito, a saber, aquel consentimiento que se deduce del acto de una persona (p. ej, la acción consistente en utilizar un sitio web se entiende que implica consentimiento para el registro de los datos del usuario con fines comerciales). También puede deducirse del silencio o de la inacción (no deseleccionar una casilla se considera consentimiento).

80. Según la Directiva, para que el consentimiento sea válido debe ser informado, libre y específico. Debe tratarse de una manifestación informada de los deseos de la persona mediante la cual consienta al tratamiento de los datos personales que le conciernan. El consentimiento debe otorgarse de manera inequívoca.

81. El consentimiento que se haya deducido de una acción y, más en particular, del silencio o la inacción no constituye por lo general un consentimiento inequívoco. No obstante, no siempre es fácil determinar qué constituye un consentimiento verdadero e inequívoco. Determinados responsables del tratamiento de datos explotan esta incertidumbre recurriendo a métodos que excluyen toda posibilidad de dar un consentimiento verdadero e inequívoco.

82. A la luz de todo lo anterior, el SEPD comparte el punto de vista de la Comisión en relación con la necesidad de precisar los límites del consentimiento y asegurarse de que únicamente el consentimiento resultante de un comportamiento no equívoco sea considerado como tal. En este contexto, el SEPD sugiere lo siguiente ([39]):

— Considerar eventualmente la posibilidad de ampliar las situaciones en las que es necesario un consentimiento expreso, limitado actualmente a los datos sensibles;

— adoptar normas adicionales para el consentimiento en un entorno virtual;

— adoptar normas adicionales relativas al consentimiento para tratar datos con fines secundarios (es decir, el tratamiento es secundario al tratamiento principal y no aparece como una evidencia);

— en un nuevo instrumento legislativo, adoptado o no por la Comisión en virtud del artículo 290 del TFUE, determinar el tipo de consentimiento requerido, por ejemplo, precisar el nivel de consentimiento en relación con el tratamiento de datos de las etiquetas RFID de los productos destinados al consumo o a otras técnicas específicas.

6.5. *La portabilidad de los datos y el derecho al olvido*

83. La portabilidad de los datos y el derecho a ser olvidado son dos nociones interrelacionadas y presentadas en la Comunicación con el fin de reforzar los derechos de los interesados. Vienen a complementar los principios ya indicados en la Directiva, que establecen el derecho del interesado a expresar una objeción al tratamiento ulterior de sus datos personales así como una obligación para el responsable del tratamiento de suprimir la información cuando ya no sea necesaria a los fines del tratamiento.

84. Estos dos nuevos conceptos tienen, ante todo, un valor añadido en el contexto de la sociedad de la información, en la que cada vez es mayor el número de datos que se almacena de manera automática y se conservan durante períodos indeterminados. En la práctica se demuestra que, incluso cuando es el propio interesado quien aporta los datos, su grado de control efectivo sobre los mismos es muy limitado, lo cual resulta aún más incuestionable a la vista de la enorme memoria que representa hoy en día Internet. Además, desde un punto de vista económico, resulta más costoso para el responsable del tratamiento suprimir los datos que conservarlos almacenados. El ejercicio de los derechos de las personas es contrario, por tanto, a la tendencia económica natural.

85. Tanto la portabilidad de los datos como el derecho al olvido podrían contribuir a inclinar la balanza a favor del interesado. La portabilidad de los datos tendría por objeto proporcionar un mayor grado de control a las personas sobre su información, mientras que el derecho al olvido garantizaría que la información desaparece automáticamente al cabo de un determinado período, incluso si el interesado no realiza ninguna acción en este sentido o desconoce que los datos fueron almacenados.

86. De manera más específica, por portabilidad de los datos se entiende la capacidad de los usuarios para modificar sus preferencias en relación con el tratamiento de sus datos, vinculados especialmente a los nuevos servicios tecnológicos. Esta posibilidad es cada vez más aplicable a los servicios que implican un almacenamiento de la información, incluidos los datos personales, como la telefonía móvil y los servicios que almacenan fotografías, correos electrónicos y otra información, utilizando en ocasiones para ello servicios de computación en nube.

87. Las personas deben tener libertad para cambiar con sencillez de proveedor y transferir sus datos personales a otro proveedor de servicios. El SEPD considera que los derechos vigentes reflejados en la Directiva 95/46/CE podrían reforzarse mediante la inclusión de un derecho de portabilidad en el contexto de los servicios de la sociedad de la información. Dicho derecho contribuiría a ayudar a las personas a obtener el acceso a su información personal mientras que, al mismo tiempo, se reforzaría la obligación de los antiguos proveedores u otros responsables de suprimir dicha información.

88. La codificación de un nuevo «derecho al olvido» garantizaría la supresión de los datos personales o la prohibición de un uso posterior de los mismos, sin necesidad de

([39]) El Grupo de Trabajo del artículo 29 trabaja en la actualidad en un dictamen sobre el «consentimiento». Dicho dictamen podría aportar otras sugerencias.

acción alguna por parte del interesado, a condición de que estos datos ya hubieran sido almacenados durante un período determinado. Dicho de otro modo, se podría atribuir a los datos una especie de fecha de caducidad. Este principio ya ha sido invocado en litigios ante los tribunales nacionales o aplicados en sectores específicos como, por ejemplo, los expedientes policiales o los antecedentes penales o disciplinarios. En virtud de algunas legislaciones nacionales, la información sobre las personas se suprime automáticamente o no se utiliza o difunde posteriormente, especialmente al cabo de un período determinado, sin necesidad de un análisis previo, caso por caso.

89. En este sentido, un nuevo «derecho al olvido» debería guardar relación con la portabilidad de los datos. Su valor añadido consiste en que eximir al interesado de todo esfuerzo o insistencia en hacer efectiva la supresión de sus datos, ya que se llevaría a cabo de un modo objetivo y automatizado. El responsable del tratamiento de los datos estaría autorizado a conservarlos únicamente en circunstancias muy concretas, en las que pueda determinarse una necesidad específica de conservarlos durante un período de tiempo más prolongado. Por tanto, el «derecho al olvido» invertiría la carga de la prueba de la persona hacia el responsable del tratamiento y constituiría un «derecho a la intimidad por defecto» establecido para el tratamiento de datos personales.

90. El SEPD considera que el derecho a ser olvidado podría ser especialmente útil en el contexto de los servicios de la sociedad de la información. La obligación de suprimir y de volver a difundir la información al cabo de un determinado período tiene sentido especialmente en los medios de comunicación o en Internet y, en particular, en las redes sociales. También resultaría útil en relación con los equipos terminales, ya que los datos almacenados en dispositivos móviles o en ordenadores se suprimirían o bloquearían de manera automática tras un período determinado, cuando ya no estén en poder de la persona. En este sentido, el derecho a ser olvidado puede interpretarse como una obligación de «intimidad mediante el diseño».

91. En resumen, el SEPD opina que la portabilidad de los datos y el derecho a ser olvidado son conceptos útiles, que merecen ser incluidos en el instrumento jurídico, aunque probablemente deberán limitarse al entorno electrónico.

6.6. *Tratamiento de los datos personales relativos a menores*

92. En la Directiva 95/46/CE no están contempladas normas particulares en relación con el tratamiento de los datos personales de menores, ello implica que no se reconoce la necesidad de protección específica, debida a la vulnerabilidad de este colectivo, y al mismo tiempo se crea inseguridad jurídica, en especial en los siguientes ámbitos:

— la obtención de datos de menores y cómo informárseles respecto a dicha obtención;

— el modo en que se obtiene el consentimiento de los menores. Al no existir normas específicas sobre el modo de obtención del consentimiento de los menores y la edad mínima para que se les considere como tales, estas materias son abordadas en el marco de la legislación nacional, que difiere entre los diferentes Estados miembros ([40]);

— el modo y las condiciones en que los menores o sus representantes legales pueden ejercer sus derechos en virtud de la Directiva.

93. El SEPD considera que los intereses particulares de los menores gozarían de mejor protección si el nuevo instrumento jurídico incluyese disposiciones adicionales, destinadas especialmente a la obtención y posterior tratamiento de los datos de menores. Dichas disposiciones específicas deberían proporcionar seguridad jurídica en este ámbito concreto y beneficiar a los responsables del tratamiento actualmente sujetos a diferentes requisitos jurídicos.

94. El SEPD sugiere incluir las siguientes disposiciones en el instrumento jurídico:

— una obligación de adaptar la información a los menores de manera que estos entiendan mejor qué significa la obtención de sus datos;

— otros requisitos de información adaptados a los menores, sobre cómo debe proporcionarse la información y posiblemente también sobre su contenido;

— una disposición específica que proteja a los menores contra la publicidad basada en el comportamiento;

— el principio de limitación a una finalidad específica debe potenciarse en relación con los datos de menores;

— no deberían obtenerse nunca determinadas categorías de datos;

— un límite de edad, por debajo del cual, la información relativa a los menores debería obtenerse, en general, únicamente con un consentimiento parental explícito y verificable;

— si es necesario el consentimiento parental, será necesario establecer normas sobre el modo de verificar la

([40]) El consentimiento se vincula normalmente a la edad en la cual el menor puede contraer obligaciones contractuales. Se trata de la edad en la que se supone que los menores han alcanzado un determinado nivel de madurez. Por ejemplo, la legislación española requiere el consentimiento parental para obtener datos de los niños menores de 14 años. A los que superen dicha edad se les considerará capacitados para consentir. En el Reino Unido, la Ley de protección de datos (*Data protection Act*) no hace referencia a ninguna edad o umbral en particular. Sin embargo, la Autoridad Británica de protección de datos ha interpretado que los niños mayores de 12 años pueden dar su consentimiento. Por el contrario, los menores de 12 años no podrán dar su consentimiento y para obtener sus datos personales será necesario obtener primero el permiso de un padre o tutor.

edad del menor, es decir, conocer que el niño es un menor y verificar el consentimiento parental. En este ámbito, la Unión Europea puede inspirarse en la experiencia de otros países, como los Estados Unidos ([41]).

6.7. *Mecanismos de recurso colectivo*

95. Reforzar en esencia los derechos de las personas no tendría sentido si no existieran mecanismos procesales eficaces para aplicar dichos derechos. En este contexto, el SEPD recomienda la introducción en la legislación europea de mecanismos de recurso colectivo para las violaciones de las normas de protección de datos. En particular, los mecanismos de recurso colectivo que facultan a grupos de ciudadanos a presentar sus demandas mediante una actuación única constituyen una herramienta muy poderosa que facilita la aplicación de las normas de protección de datos ([42]). Esta innovación también cuenta con el apoyo de las autoridades encargadas de la protección de datos en el documento del Grupo de Trabajo sobre la protección de la intimidad en el futuro.

96. En casos menos notorios, es poco probable que las víctimas de una violación de las normas de protección de datos interpongan demandas individuales contra los responsables del tratamiento, en razón de los costes, demoras, incertidumbres, riesgos y cargas a los que se verían expuestas. Estas dificultades podrían superarse o atenuarse sustancialmente si se introdujera un sistema de recurso colectivo, que facultase a las víctimas de violaciones para unir sus reclamaciones individuales en una actuación única. El SEPD también aboga por habilitar a las entidades cualificadas, como las asociaciones de consumidores u organismos públicos, a presentar demandas en representación de las víctimas de violaciones de la protección de datos. Estas demandas existirían sin perjuicio del derecho del interesado a interponer un recurso individual.

97. Las demandas colectivas no solo son importantes para garantizar una indemnización total u otras vías de reparación, sino que también poseen una función disuasoria. El riesgo de incurrir en costosos daños colectivos resultantes de dichas actuaciones multiplicaría los incentivos de los responsables del tratamiento para garantizar el cumplimiento de una manera eficaz. A este respecto, la mejora de las actividades de control de aplicación de las reglas por parte de particulares sirviéndose de mecanismos de recurso colectivo vendría a completar las medidas de control de los organismos públicos.

98. La Comunicación no adopta una postura a este respecto. El SEPD es consciente del debate en curso a nivel europeo sobre la introducción de recursos colectivos para los consumidores. También es consciente de los posibles excesos que estos mecanismos pueden llevar aparejados, atendiendo a la experiencia de otros ordenamientos jurídicos. Sin embargo, estos factores no constituyen, en su opinión, un argumento suficiente para rechazar o posponer la introducción de dichos mecanismos en la legislación sobre protección de datos, a la vista de los beneficios que podría implicar ([43]).

7. **Reforzar el papel de las organizaciones y responsables del tratamiento**

7.1. *General*

99. El SEPD considera que un instrumento jurídico moderno, además de reforzar los derechos de las personas, debe incluir las herramientas necesarias para potenciar la responsabilidad de los responsables del tratamiento. Más concretamente, el marco debe incluir incentivos para que los responsables del tratamiento del sector privado o público incluyan de manera proactiva medidas de protección de los datos en sus procesos empresariales. Estas herramientas serían, en primer lugar, útiles ya que, tal como se ha señalado anteriormente, los progresos tecnológicos derivados del marcado incremento en la obtención, la utilización y posterior transferencia de los datos personales, causante de un aumento de las amenazas para la intimidad y la protección de los datos personales de las personas, deben compensarse de manera eficaz. En segundo lugar, el marco actual carece — salvo en un limitado número de disposiciones bien definidas (véase a continuación) — de herramientas, por lo que los responsables del tratamiento pueden adoptar un enfoque *reactivo* en relación con la protección de datos y la intimidad, y actuar únicamente después de que se haya manifestado un problema. Este enfoque se pone de manifiesto en las estadísticas, que demuestran que las prácticas de cumplimiento inadecuado y las pérdidas de datos son problemas recurrentes.

100. En opinión del SEPD, el marco existente no basta para proteger los datos personales de manera eficaz en virtud de las condiciones presentes y futuras. Cuanto mayor es el riesgo, mayor es la necesidad de aplicar medidas concretas que protejan la información a nivel práctico y proporcionen una protección eficaz. A menos que estas medidas proactivas encuentren aplicación en la práctica, continuarán produciéndose errores, contratiempos y negligencias, comprometiendo así la protección de la intimidad individual en una sociedad cada vez más digitalizada. Para llevar todo ello a la práctica, el SEPD propone las siguientes medidas.

7.2. *Reforzar la responsabilidad de los responsables del tratamiento de datos*

101. El SEPD recomienda introducir una nueva disposición en el instrumento jurídico que obligue a los responsables del tratamiento de datos a aplicar medidas adecuadas y eficaces para poner en práctica los principios y las obligaciones de dicho instrumento y demostrar dicha aplicación siempre que se les inste a hacerlo.

([41]) En los Estados Unidos, la Ley de protección de la intimidad en línea de los menores (COPPA, por sus siglas en inglés) exige a los operadores de sitios web comerciales o de los servicios en línea dirigidos a menores de 13 que obtengan el consentimiento parental antes de obtener datos personales, y a los operadores de sitios web para el público en general que tengan un conocimiento real de que determinados visitantes son menores.

([42]) Véase asimismo el Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos, DO C 255 de 27.10.2007, p. 10.

([43]) Algunas legislaciones nacionales ya prevén mecanismos similares.

102. Este tipo de disposición no es absolutamente novedosa. El artículo 6, apartado 2, de la Directiva 95/46/CE hace referencia a los principios relativos a la calidad de los datos y establece que «corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1». Asimismo, el artículo 17, apartado 1, obliga a los responsables del tratamiento a aplicar medidas, tanto de carácter técnico como organizativo. Sin embargo, estas disposiciones poseen un ámbito de aplicación limitado. La introducción de una disposición general relativa a la responsabilidad estimularía a los responsables a adoptar medidas proactivas con el fin de cumplir con todos los elementos de la legislación sobre protección de datos.

103. Como consecuencia de una disposición sobre la responsabilidad, se obligaría a los responsables del tratamiento de datos a aplicar mecanismos internos y sistemas de control que garanticen el cumplimiento de los principios y las obligaciones del marco. Ello exigiría, por ejemplo, la participación del personal gerente en las políticas de protección de datos, planificar procedimientos para garantizar una identificación adecuada de todas las operaciones de tratamientos de datos, disponer de políticas de protección de datos vinculantes que deberían revisarse y actualizarse de manera continua con el fin de cubrir las nuevas operaciones, cumplir los principios de calidad de los datos, notificación, seguridad, acceso, etc. También obligaría a que los responsables del tratamiento conserven las pruebas con el fin de demostrar el debido cumplimiento cuando las autoridades así lo soliciten. En determinados casos, demostrar a la ciudadanía el cumplimiento de las normas debería tener en general un carácter obligatorio y podría llevarse a cabo, por ejemplo, exigiendo a los responsables del tratamiento la inclusión de la protección de datos en los informes públicos (anuales), cuando dichos informes sean obligatorios por otros motivos.

104. Obviamente, los tipos de medidas internas y externas que deben aplicarse habrán de ser adecuadas y depender de los hechos y circunstancias de cada caso particular. Es diferente que el responsable trate algunos centenares de registros de clientes que consisten simplemente en nombres y direcciones o que dicho responsable trate registros de millones de pacientes, en particular sus historiales clínicos. También es aplicable a los modos específicos en que debe evaluarse la eficacia de las medidas. Es necesaria la proporcionalidad.

105. El instrumento jurídico completo y global de protección de los datos no debería establecer los requisitos específicos de responsabilidad sino únicamente sus elementos esenciales. La Comunicación prevé determinados elementos, acogidos con gran satisfacción, con el fin de reforzar la responsabilidad de los responsables del tratamiento. En concreto, el SEPD aboga porque sean obligatorias las evaluaciones de impacto sobre la intimidad, con arreglo a determinadas condiciones límite.

106. Asimismo, el SEPD recomienda que se deleguen poderes a la Comisión con arreglo al artículo 290 del TFUE con el fin de cumplir los requisitos básicos necesarios para cumplir con el estándar de responsabilidad. El uso de estos poderes aumentaría la seguridad jurídica de los responsables del tratamiento y armonizaría el cumplimiento en toda la Unión Europea. Para la elaboración de dichos instrumentos específicos, deberá consultarse al Grupo de Trabajo del «artículo 29» y al SEPD.

107. Por último, las medidas concretas de responsabilidad requeridas de los responsables del tratamiento podrían imponerse igualmente por parte de las autoridades encargadas de la protección de datos en el marco del control de aplicación de las normas. Para ello, se debería otorgar a las autoridades encargadas de la protección de datos nuevos poderes que les permitan imponer medidas de reparación o sanciones. Los ejemplos deberían incluir el establecimiento de programas de cumplimiento interno, implantar la intimidad mediante el diseño en productos y servicios específicos, etc. Las medidas correctoras impuestas deberían ser apropiadas, proporcionadas y eficaces para garantizar el cumplimiento de las normas jurídicas aplicables y ejecutables.

7.3. Intimidad mediante el diseño

108. El concepto de intimidad mediante el diseño hace referencia a la integración de la protección de datos y la protección de la intimidad desde la fase de concepción de nuevos productos, servicios y procedimientos que implican el tratamiento de datos personales. En opinión del SEPD, la intimidad mediante el diseño constituye un elemento del principio de responsabilidad. Por lo tanto, se exigiría asimismo a los responsables del tratamiento demostrar que han aplicado la intimidad mediante el diseño, cuando sea necesario. Recientemente, la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Protección de la Intimidad emitió una resolución en la que se reconocía la intimidad mediante el diseño como componente esencial de la protección de la intimidad ([44]).

109. La Directiva 95/46/CE incluye algunas disposiciones que promueven la intimidad mediante el diseño ([45]), pero no reconoce explícitamente dicha obligación. Al SEPD le complace que la Comunicación defienda la intimidad mediante el diseño como un instrumento para garantizar el cumplimiento de las normas de protección de datos. Sugiere que se incluya una disposición vinculante que establezca la obligación de «intimidad mediante el

([44]) Resolución relativa a la intimidad mediante el diseño, adoptada en la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Jerusalén 27-29 de octubre de 2010.

([45]) La Directiva incluye disposiciones que, de forma indirecta y en distintas situaciones, piden que se aplique la intimidad mediante el diseño. En particular, el artículo 17 exige que los responsables del tratamiento de datos apliquen las medidas técnicas y de organización adecuadas para evitar el tratamiento ilícito de datos. La Directiva sobre privacidad es más explícita. Su artículo 14, apartado 3, establece que «cuando proceda, se podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales, de conformidad con la Directiva 1999/5/CE y la Decisión 87/95/CEE del Consejo, de 22 de diciembre de 1986, relativa a la normalización en el campo de la tecnología de la información y de las telecomunicaciones».

diseño», que podría estar basada en el tenor del considerando 46 de la Directiva 95/46/CE. Más concretamente, la disposición exigiría explícitamente que los responsables del tratamiento de datos aplicasen medidas técnicas y de organización, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los propios tratamientos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado ([46]).

110. En virtud de dicha disposición, podría exigirse a los responsables del tratamiento de datos, entre otras cosas, que se aseguren de que los sistemas de tratamiento de datos afecten a tan pocos datos personales como sea posible, que apliquen parámetros de privacidad por defecto, por ejemplo en las redes sociales, a fin de impedir a otros usuarios el acceso por defecto a los perfiles de otras personas y que apliquen herramientas que permitan a los usuarios proteger mejor sus datos personales (por ejemplo, controles de acceso, encriptación).

111. Las ventajas de incluir una referencia más explícita a la intimidad mediante el diseño pueden resumirse en los siguientes términos:

— destacaría la importancia del propio principio, como instrumento para garantizar que los procesos, productos y servicios se diseñan desde el principio teniendo en cuenta la intimidad;

— reduciría los atentados contra la protección de la intimidad y minimizaría las obtenciones innecesarias de datos, habilitando a las personas a tomar decisiones decisivas en relación con sus datos personales;

— evitaría tener que colocar «parches» a posteriori en un afán de solucionar problemas que pueden resultar difíciles, sino imposibles, de solucionar;

— facilitaría asimismo la aplicación y ejecución efectivas de dicho principio por parte de las autoridades encargadas de la protección de datos.

112. El efecto combinado de esta obligación se traduciría en una mayor demanda de productos y servicios concebidos de acuerdo con este principio, lo que incentivaría a la industria a responder a esta demanda. Convendría, además, crear una obligación diferenciada dirigida a los diseñadores y fabricantes de nuevos productos y servicios con un posible impacto sobre la protección de datos y la protección de la intimidad. El SEPD sugiere que se incluya dicha obligación diferenciada, susceptible de permitir a los responsables del tratamiento de datos cumplir con sus propias obligaciones.

113. La codificación del principio de intimidad mediante el diseño podría complementarse con una disposición que estableciese requisitos específicos: por ejemplo, requisitos de intimidante mediante el diseño relativos a los mecanismos para establecer la capacidad del usuario, que deberán adoptarse en virtud de dicho principio.

114. Asimismo, el SEPD recomienda que se deleguen poderes a la Comisión con arreglo al artículo 290 del TFUE para añadir, en su caso, los requisitos básicos de intimidad mediante el diseño a los productos y servicios seleccionados. El uso de estos poderes aumentaría la seguridad jurídica de los responsables del tratamiento y armonizaría el cumplimiento en toda la Unión. Para la elaboración de dichos instrumentos específicos, deberá consultarse al Grupo de Trabajo del artículo 29 y al SEPD (véase en este sentido el punto 106 sobre responsabilidad).

115. Por último, debería concederse a las autoridades encargadas de la protección de los datos la potestad de imponer medidas de reparación o sanciones, con arreglo a condiciones restrictivas similares, como ya se ha mencionado en el punto 107, cuando los responsables del tratamiento no hayan logrado claramente adoptar medidas concretas en los casos en que fueran precisas.

7.4. *Servicios de certificación*

116. La comunicación reconoce la necesidad de examinar la creación de regímenes europeos de certificación para los productos y servicios que sean conformes a las normas de protección de la intimidad. El SEPD apoya totalmente este objetivo y sugiere incluir una disposición que establezca dicha creación y los eventuales efectos en toda la Unión, que podrá desarrollarse posteriormente en la legislación complementaria. La disposición debería complementar las disposiciones relativas a la responsabilidad y a la intimidad mediante el diseño.

117. Los regímenes voluntarios de certificación permitirían verificar que un responsable del tratamiento de datos ha adoptado medidas para cumplir lo dispuesto en el instrumento jurídico. Asimismo, es probable que los responsables del tratamiento de datos, o incluso los productos o servicios, que dispongan de una marca de certificación, obtengan una ventaja competitiva frente al resto. Dichos regímenes también ayudarían a las autoridades encargadas de la protección de datos en su papel de supervisión y ejecución.

8. **Globalización y Derecho aplicable**

8.1. *Necesidad clara de una mayor coherencia en materia de protección*

118. Como se ha mencionado en el capítulo 2, la transferencia de datos personales más allá de las fronteras de la Unión ha crecido de manera exponencial como consecuencia del desarrollo de las nuevas tecnologías, el papel de las empresas multinacionales y la creciente influencia de los gobiernos en el tratamiento y el intercambio de datos personales a escala internacional. Este es uno de los principales motivos que justifican la revisión del marco jurídico actual. Por consiguiente, este es uno de los ámbitos en los que el SEPD pide que se sea ambicioso y eficaz, ya que existe una necesidad clara de una protección más coherente cuando los datos son tratados fuera de la Unión.

([46]) En virtud del marco actual, el considerando 46 anima a los responsables del tratamiento a aplicar dichas medidas aunque lo establecido en un considerando no tiene fuerza vinculante.

8.2. *Invertir en normas internacionales*

119. En opinión del SEPD es necesaria una mayor inversión en la elaboración de normas internacionales. En relación con el nivel de protección de los datos personales en todo el mundo, una mayor armonización aclararía de manera considerable la esencia de los principios que deben cumplirse y las condiciones aplicables a las transferencias de datos. Estas normas mundiales deberían conciliar el requisito de un elevado nivel de protección de datos, incluidos los elementos esenciales de la protección de datos en la Unión, con las especificidades de cada espacio regional.

120. El SEPD apoya la ambiciosa labor desarrollada hasta el momento en el marco de la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad para elaborar y difundir las denominadas «normas de Madrid», con el fin de integrarlas en un instrumento vinculante y probablemente iniciar una conferencia intergubernamental ([47]). Pide a la Comisión que adopte las iniciativas necesarias para facilitar la realización de este objetivo.

121. En opinión del SEPD, también es importante garantizar la coherencia entre esta iniciativa de normas internacionales, la revisión actual del marco de protección de datos de la Unión y otras disposiciones, como la actual revisión de las Directrices de la OCDE relativas a la privacidad y las del Convenio nº 108 del Consejo de Europa, que está abierto a la firma por parte de terceros países (véase asimismo el punto 17). El SEPD considera que la Comisión juega un papel específico en esta cuestión, a la hora de especificar el modo en que promoverá esta coherencia en las negociaciones en la OCDE y el Consejo de Europa.

8.3. *Clarificar los criterios en materia de derecho aplicable*

122. Dado que no es fácil alcanzar una coherencia total, subsistirá, al menos en el futuro inmediato, cierta diversidad entre las legislaciones dentro de la Unión y, a fortiori, más allá de las fronteras de la Unión. El SEPD considera que un nuevo instrumento jurídico deberá aclarar los criterios que determinan la legislación aplicable y asegurar mecanismos racionales para los flujos de datos, así como la responsabilidad de los actores implicados en dichos flujos.

123. En primer lugar, el instrumento jurídico deberá garantizar que la legislación de la Unión resulte aplicable cuando se tratan datos personales fuera de las fronteras de la Unión, y en aquellos casos en los que está justificada la aplicación de dicha legislación. Un ejemplo de esta necesidad son los servicios de computación en nube no europeos destinados a residentes de la Unión. En entornos en los que los datos no se encuentran físicamente almacenados ni tratados en un lugar fijo, donde los proveedores de servicios y los usuarios ubicados en diferentes países interfieren sobre los datos, es muy difícil identificar al responsable del cumplimiento de los principios de protección de datos. Se proporcionan orientaciones, en especial por parte de las autoridades encargadas de la protección de datos, sobre el modo de interpretar y aplicar la Directiva 95/46/CE en dichos casos, aunque dichas orientaciones no bastan para garantizar la seguridad jurídica en este nuevo entorno.

124. En el territorio de la Unión Europea, el Grupo de Trabajo del artículo 29 ha insistido, en un dictamen reciente, en la necesidad de una mayor precisión del marco jurídico y de un criterio simplificado para determinar la legislación aplicable ([48]).

125. En opinión del SEPD, la opción preferida sería elaborar el instrumento jurídico en un reglamento, lo que se traduciría en la aplicación de normas idénticas aplicables en todos los Estados miembros. Servirse de un reglamento permitiría rebajar la necesidad de determinar el derecho aplicable. Este es uno de los motivos por los que el SEPD es firmemente favorable a la adopción de un reglamento. Sin embargo, un reglamento también permitiría un cierto margen de maniobra para los Estados miembros. Si se conserva un cierto margen de maniobra significativo en el nuevo instrumento, el SEPD apoyaría la sugerencia del Grupo de Trabajo de cambiar la situación actual que implica una aplicación distributiva de las distintas legislaciones nacionales a un sistema basado en una aplicación centralizada de una legislación única en todos los Estados miembros donde el responsable del tratamiento se encuentre ubicado. Pide asimismo mayor cooperación y coordinación entre las autoridades encargadas de la protección de datos en los asuntos y reclamaciones transnacionales (véase el capítulo 10).

8.4. *Simplificar los mecanismos para los flujos de datos*

126. Debe tenerse en cuenta la necesidad de coherencia y de un elevado nivel de referencia no solo respecto de los principios globales de protección de datos sino también respecto de las transferencias internacionales. El SEPD apoya totalmente el objetivo de la Comisión de racionalizar los procedimientos actuales de transferencia internacional de datos y garantizar un enfoque más uniforme y coherente respecto a los terceros países y las organizaciones internacionales.

127. El mecanismo de los flujos de datos incluye tanto las transferencias del sector privado, en especial a través de cláusulas contractuales o normas vinculantes para las empresas, como las transferencias entre las autoridades públicas. Las normas vinculantes para las empresas son uno de los elementos para los que sería deseable la existencia de un enfoque más coherente y racionalizado. El SEPD recomienda abordar las condiciones de las normas vinculantes para las empresas de un modo explícito en un nuevo instrumento jurídico ([49]):

— reconociendo explícitamente que las normas vinculantes para las empresas son herramientas que proporcionan las adecuadas garantías;

— estableciendo los elementos y condiciones principales para la adopción de dichas normas;

([47]) Tal como sugiere la Resolución sobre Normas Internacionales, adoptada en la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Jerusalén 27-29 de octubre de 2010.

([48]) Dictamen 8/2010 del Grupo de Trabajo del artículo 29 relativo a la legislación aplicable, WP 179.

([49]) En relación con las transferencias internacionales, véase asimismo el capítulo 8 del dictamen.

— estableciendo procedimientos de cooperación para la adopción de normas vinculantes para las empresas, incluidos los criterios de selección de una autoridad de supervisión principal (ventanilla única).

9. **Ámbito policial y judicial**

9.1. *Instrumento general*

128. La Comisión ha subrayado repetidamente la importancia de reforzar la protección de datos en el contexto policial y de prevención de la delincuencia, en el que el intercambio y la utilización de información personal se ha intensificado significativamente. Asimismo, el Programa de Estocolmo, aprobado por el Consejo de Europa, menciona la necesidad de un régimen sólido de gestión de los datos como principal requisito previo para la Estrategia de Gestión de la Información de la UE en este ámbito ([50]).

129. La revisión del marco general de protección de datos es la ocasión perfecta para avanzar en este sentido, en particular desde el momento en que la Comunicación describe acertadamente la Decisión Marco 2008/977 como inadecuada ([51]).

130. El SEPD razonó en la sección 3.2.5 del presente dictamen el motivo por el que el ámbito de cooperación policial y judicial debe incluirse en el instrumento general. La inclusión del ámbito policial y judicial comporta una serie de beneficios adicionales, lo que significa que las normas ya no se aplicarán únicamente a los intercambios transfronterizos de datos ([52]), sino también al tratamiento nacional. También se garantizará mejor una protección adecuada en el intercambio de datos personales con terceros países, también en relación con los acuerdos internacionales. Además, las autoridades encargadas de la protección de datos dispondrán frente a las autoridades policiales y judiciales de las mismas facultades, armonizadas, de que disponen respecto de otros responsables del tratamiento. Finalmente, el actual artículo 13, que establece que los Estados miembros podrán adoptar legislación específica para limitar el alcance de las obligaciones y los derechos previstos en virtud de un instrumento general en caso de determinados intereses públicos, deberá ser aplicado de manera tan restrictiva como se aplica en otros ámbitos. En particular, las salvaguardias específicas establecidas en virtud de un instrumento general en este ámbito deberán respetar asimismo la legislación nacional adoptada en el ámbito de la cooperación policial y judicial.

([50]) Véase el Dictamen del Supervisor Europeo de Protección de Datos de 30 de septiembre de 2010 sobre la comunicación de la Comisión al Parlamento Europeo y al Consejo — «Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia», apartados 9-19.

([51]) Véase la sección 3.2.5.

([52]) Este es actualmente el limitado ámbito de aplicación de la Decisión Marco 2008/977.

9.2. *Normas específicas adicionales en materia policial y judicial*

131. Sin embargo, dicha inclusión no excluye la existencia de normas especiales y de excepciones, que tienen debidamente en cuenta las especificidades de este sector, con arreglo a la Declaración 21 anexa al Tratado de Lisboa. Pueden preverse limitaciones a los derechos de los interesados aunque deberán ser necesarias, proporcionadas y no alterar los elementos esenciales del propio derecho. En este contexto debe destacarse que la Directiva 95/46/CE, incluido su artículo 13, se aplica actualmente con fines represivos en diferentes ámbitos (p. ej., fiscalidad, aduanas, lucha contra el fraude) que no difieren esencialmente de muchas de las actividades en el ámbito policial y judicial.

132. Además, deben aplicarse salvaguardias específicas, para compensar al interesado concediéndole una protección complementaria en un ámbito en que el tratamiento de datos personales puede ser más invasivo.

133. A la luz de lo anterior, el SEPD considera que el nuevo marco debe incluir, al menos, los siguientes elementos, con arreglo al Convenio nº 108 y a la Recomendación nº R (87) 15:

— una distinción entre las diferentes categorías de datos y ficheros, en función de su precisión y fiabilidad, respetando el principio de que los datos basados en hechos deben distinguirse de los datos basados en opiniones o valoraciones personales;

— una distinción entre las diversas categorías de interesados (sospechosos, víctimas, testigos, etc.) y de ficheros (temporales, permanentes y ficheros de explotación de datos); deben preverse condiciones y salvaguardias específicas para el tratamiento de los datos de personas no sospechosas;

— mecanismos para garantizar la comprobación y rectificación periódicas con el fin de salvaguardar la calidad de los datos tratados;

— pueden elaborarse disposiciones o salvaguardias específicas en relación con el tratamiento (cada vez más relevante) de datos biométricos y genéticos en el ámbito policial. Su utilización debe limitarse únicamente a los casos en los que no se disponga de otros medios menos invasivos que puedan garantizar el mismo efecto ([53]);

— condiciones para las transferencias de datos personales a autoridades no competentes y partes privadas, así como el acceso y posterior utilización de los datos obtenidos por partes privadas, por parte de las autoridades policiales.

([53]) Véase, en este sentido, el Documento del Grupo de Trabajo sobre el futuro de la protección de la vida privada, punto 112.

9.3. *Regímenes sectoriales específicos en materia de protección de datos*

134. De acuerdo con la comunicación, «la Decisión Marco no sustituye a los diversos instrumentos legislativos específicamente sectoriales adoptados a escala de la UE en el ámbito de la cooperación policial y judicial en materia penal, en particular, los que regulan el funcionamiento de Europol, Eurojust, el Sistema de Información de Schengen (SIS) y el Sistema de Información Aduanero (SIA), que prevén regímenes especiales de protección de datos o que suelen remitirse a los instrumentos de protección de datos del Consejo de Europa».

135. En opinión del SEPD, un nuevo marco jurídico debería ser, en la medida de lo posible, claro, simple y coherente. Cuando existe una proliferación de distintos regímenes aplicables, por ejemplo, Europol, Eurojust, el sistema SIS y de la Decisión Prüm, el cumplimiento de las normas sigue siendo complicado, o más complicado aún. Este es uno de los motivos por los que el SEPD es favorable a un instrumento jurídico global para todos los sectores.

136. Sin embargo, el SEPD entiende que alinear las normas de los distintos sistemas exigirá una labor considerable, que debe llevarse a cabo atentamente. El SEPD considera que un enfoque gradual, como se menciona en la Comunicación, tiene sentido siempre que el compromiso de garantizar un alto nivel de protección de datos de manera coherente y eficaz siga siendo claro y diáfano. Más concretamente:

— En una primera fase, el instrumento jurídico general de protección de datos deberá aplicarse a todo tipo de tratamiento en el ámbito de la cooperación policial y judicial, incluidos los ajustes en el ámbito de la policía y la justicia (tal como se menciona en el punto 9.2).

— En una segunda fase, los regímenes específicos sectoriales de protección de datos deben alinearse con el instrumento general. La Comisión debe comprometerse a adoptar propuestas para esta segunda fase, en un breve plazo y específico.

10. **Autoridades encargadas de la protección de datos y la cooperación entre las mismas**

10.1. *Reforzar el papel de las autoridades encargadas de la protección de datos*

137. El SEPD apoya plenamente el objetivo de la Comisión en el sentido de abordar el estatuto de las autoridades encargadas de la protección de datos y, más concretamente, potenciar su independencia, recursos y facultades represivas.

138. El SEPD insiste asimismo en la necesidad de clarificar en el nuevo instrumento jurídico la noción básica de independencia de las autoridades encargadas de la protección de datos. El Tribunal de Justicia Europeo ha adoptado recientemente una resolución sobre esta cuestión en el asunto C-518/07 ([54]), en el que hace hincapié en que la independencia significa inexistencia de toda influencia externa. Las autoridades de protección de datos no deben solicitar instrucciones a nadie. El SEPD sugiere explícitamente que se codifiquen legalmente dichos elementos de independencia.

139. Para desarrollar sus funciones, las autoridades encargadas de la protección de datos, deben contar con los suficientes recursos humanos y económicos. El SEPD propone incluir este requisito en el instrumento jurídico ([55]). Finalmente, destaca la necesidad de asegurarse de que las autoridades dispongan de plenas potestades de investigación y de imposición de las medidas y sanciones disuasorias y de reparación que resulten pertinentes, lo que aumentaría la seguridad jurídica de los interesados y de los responsables del tratamiento de datos.

140. El refuerzo de la independencia, los recursos y los poderes de las autoridades encargadas de la protección de datos debe ser paralelo al refuerzo de la cooperación a nivel multilateral, especialmente a la luz del creciente número de cuestiones de protección de datos a nivel de la Unión. Obviamente, la principal infraestructura que debe utilizarse para esta cooperación es el Grupo de Trabajo del artículo 29.

10.2. *Reforzar el papel del Grupo de Trabajo*

141. La historia demuestra que, desde sus inicios en 1997 hasta hoy, el funcionamiento del grupo ha evolucionado. El Grupo ha evolucionado hacia una mayor independencia y, en la práctica, ya no puede calificarse simplemente como un simple grupo de trabajo consultivo de la Comisión. El SEPD sugiere otras mejoras en el funcionamiento del Grupo de Trabajo, particularmente las relacionadas con su infraestructura y su independencia.

142. El SEPD considera que la fuerza del grupo está intrínsecamente vinculada a la independencia y las facultades de sus miembros. En el nuevo marco jurídico, debería garantizarse la autonomía del Grupo de Trabajo, de conformidad con los criterios desarrollados por el Tribunal de Justicia Europeo en el asunto C-518/07 para la total independencia de las autoridades encargadas de la protección de datos. El SEPD considera asimismo que debe dotarse al Grupo de Trabajo de los recursos y el presupuesto necesarios, así como reforzar la secretaría, con el fin de brindar apoyo a sus aportaciones.

143. En relación con la secretaría del Grupo de Trabajo, el SEPD valora positivamente el hecho de que se encuentre adscrita a la Unidad de Protección de Datos de la Dirección General de Justicia, con la ventaja de que, de este modo, el Grupo de Trabajo puede beneficiarse de unos contactos eficaces y flexibles y de información actualizada sobre los avances en materia de protección de datos. Por otro lado, el SEPD cuestiona el hecho de que la Comisión (y Unidad específica) sea a la vez miembro, secretaría y destinatario de los dictámenes del Grupo de Trabajo, lo que justificaría una mayor independencia de la secretaría. El SEPD anima a la Comisión a que valore, en estrecha consulta con las partes involucradas, el mejor modo de garantizar esta independencia.

([54]) Asunto C-518/07, *Comisión/Alemania*, todavía no publicado en la Recopilación.

([55]) Véase, por ejemplo, el artículo 43, apartado 2, del Reglamento (CE) nº 45/2001, que incluye dicho requisito para el SEPD.

144. Por último, potenciar las facultades de las autoridades encargadas de la protección de datos obliga asimismo a dotar al Grupo de Trabajo de mayores facultades, con una estructura que incluya mejores normas y salvaguardias, así como mayor transparencia. Esto se llevará a cabo tanto para el papel consultivo como para el papel de aplicación de la ley.

10.3. *El papel consultivo del Grupo de Trabajo*

145. Las opiniones del Grupo de Trabajo deben aplicarse de manera eficaz en relación con su papel consultivo respecto de la Comisión, especialmente en relación con la interpretación y la aplicación de los principios de la Directiva y otros instrumentos de protección de datos, es decir, garantizar el carácter autorizado de las opiniones del Grupo de Trabajo. Entre las autoridades encargadas de la protección de datos es necesario que exista un mayor debate para identificar el modo de incluir lo anterior en el instrumento jurídico.

146. El SEPD recomienda soluciones que proporcionen a los dictámenes del Grupo de Trabajo un carácter más autorizado, sin modificar sustancialmente su modo de funcionamiento. El SEPD sugiere incluir una obligación para las autoridades encargadas de la protección de datos y para la Comisión de tener plenamente en cuenta los dictámenes y posiciones comunes adoptadas por el Grupo de Trabajo, sobre la base del modelo adoptado para las posiciones del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) ([56]). Además, el nuevo instrumento jurídico podría conceder al Grupo de Trabajo la función explícita de adoptar «recomendaciones interpretativas». Estas soluciones alternativas proporcionarían una mayor fuerza a las posiciones del Grupo de Trabajo, incluso ante los tribunales.

10.4. *Aplicación coordinada del marco legal por el Grupo de Trabajo*

147. En virtud del presente marco, la aplicación de la legislación relativa a la protección de datos en los Estados miembros queda en manos de las 27 autoridades encargadas de la protección de datos, con escasa coordinación en lo relativo a la resolución de determinados casos. En aquellos casos en los que se ven implicados más de un Estado miembro o cuya dimensión es claramente global, este hecho multiplica los costes para las empresas, que se ven obligadas a tratar con distintas autoridades públicas para la misma actividad y aumenta el riesgo de que exista una aplicación incoherente: podría darse el caso excepcional de que idénticas actividades de tratamiento pudieran ser consideradas lícitas por una de las autoridades encargadas de la protección de datos y estar prohibidas por otra.

148. Algunos casos revisten una dimensión estratégica que obliga a un planteamiento centralizado. El Grupo de Trabajo del artículo 29 facilita la coordinación y las acciones de aplicación de la ley entre las autoridades encargadas de la protección de datos ([57]) en las principales cuestiones de protección de datos que tienen repercusiones internacionales. Este fue el caso de las redes sociales y los motores de búsqueda ([58]), así como de los controles coordinados desarrollados por los distintos Estados miembros sobre cuestiones relativas a las telecomunicaciones y los seguros de salud.

149. Existen, no obstante, límites para las medidas de ejecución que el Grupo de Trabajo puede adoptar en virtud del presente marco. El Grupo de Trabajo puede adoptar posiciones comunes, pero no existe ningún instrumento que garantice en la práctica la aplicación efectiva de estas posiciones.

150. El SEPD propone incluir disposiciones complementarias en el instrumento jurídico que puedan avalar una aplicación coordinada del marco legal, en concreto:

— la obligación de garantizar que las autoridades encargadas de la protección de datos y la Comisión tengan plenamente en cuenta los dictámenes y posiciones comunes adoptadas por el Grupo de Trabajo del artículo 29 ([59]);

— la obligación de que las autoridades encargadas de la protección de datos cooperen lealmente entre ellas y con la Comisión y el Grupo de Trabajo del artículo 29 ([60]). Como ilustración práctica de dicha cooperación leal, podría instaurarse un procedimiento en virtud del cual las autoridades encargadas de la protección de datos informen a la Comisión o al Grupo de Trabajo en caso de medidas de ejecución forzosa con un componente transfronterizo, por analogía con el procedimiento aplicable en el presente marco en lo que se refiere a las decisiones relativas a la adecuación a escala nacional;

— especificar las normas de votación con el fin de potenciar el compromiso, por parte de las autoridades encargadas de la protección de datos, de ejecutar las decisiones del Grupo de Trabajo. Cabría prever disposiciones en virtud de las cuales el Grupo de Trabajo

([56]) Reglamento (CE) nº 1211/2009 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por el que se establece el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) y la Oficina, DO L 337 de 18.12.2009, p. 1.

([57]) Además del Grupo de Trabajo del artículo 29, la Conferencia Europea de Autoridades de Protección de Datos creó hace unos diez años un taller permanente destinado a resolver de manera coordinada las reclamaciones transfronterizas. Aunque este taller supone un innegable valor añadido en lo referente al intercambio de personal de las autoridades de protección de datos y ofrece una red fiable de puntos de contacto, no puede considerarse un mecanismo de coordinación de la toma de decisiones.

([58]) Véanse las cartas del Grupo de Trabajo del artículo 29 con fecha de 12 de mayo de 2010 y de 26 de mayo de 2010, publicadas en el sitio web del Grupo de Trabajo del artículo 29 (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) Como se ha indicado anteriormente, se establece una obligación similar en el Reglamento (CE) nº 1211/2009 que especifica las funciones del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE).

([60]) Véase, a este respecto, el artículo 3 del Reglamento (CE) nº 1211/2009, citado anteriormente.

habría de decidir sobre la base del consenso y, en caso de que no fuera posible dicho consenso, se adoptasen medidas de ejecución únicamente por mayoría cualificada. Además, cabría prever un considerando en virtud del cual las autoridades encargadas de protección de datos que emitan un voto positivo en relación con un documento tengan la obligación o el compromiso político de aplicarlo a escala nacional.

151. El SEPD desearía formular una reserva en relación con la introducción de medidas más vigorosas, como la de dotar de carácter vinculante a las posiciones del Grupo de Trabajo del artículo 29. Esto socavaría la independencia de las autoridades encargadas de la protección de datos individuales, independencia que debe ser garantizada por los Estados miembros en virtud del Derecho nacional. En caso de que las decisiones del Grupo de Trabajo repercutiesen directamente sobre terceros, como los responsables del tratamiento de datos, deberán preverse nuevos procedimientos que contemplen salvaguardias como la transparencia y la compensación, incluida la posibilidad de presentar recurso ante el Tribunal de Justicia Europeo.

10.5. *Cooperación entre el SEPD y el Grupo de Trabajo*

152. También el procedimiento de cooperación entre el SEPD y el Grupo de Trabajo es susceptible de admitir mejoras. El SEPD es miembro del Grupo de Trabajo, y contribuye dentro del grupo a las posiciones adoptadas en relación con las principales evoluciones estratégicas de la Unión Europea, al tiempo que garantiza la coherencia de sus propias posiciones. El SEPD destaca el creciente número de cuestiones relacionadas con la protección de la intimidad, tanto en el sector público como en el privado, y con implicaciones a escala nacional en muchos Estados miembros, en las que el Grupo de Trabajo juega un papel específico.

153. Al SEPD le corresponde la misión complementaria de asesorar sobre evoluciones en el contexto de la Unión Europea, misión que debería mantenerse. Como organismo europeo, ejerce su competencia consultiva en relación con las instituciones de la Unión Europea de la misma forma que las autoridades encargadas de la protección de datos aconsejan a sus gobiernos.

154. El SEPD y el Grupo de Trabajo actúan desde una perspectiva diferente aunque complementaria. Por todas estas razones, es necesario conservar y quizá incluso mejorar la coordinación entre el Grupo de Trabajo y el SEPD, para asegurarse de que colaboran juntos en relación con las principales cuestiones que afectan a la protección de datos, por ejemplo, coordinando las agendas de manera regular ([61]), y garantizando la transparencia en aquellas cuestiones que revisten un carácter más nacional o más específico de la Unión.

155. En la actual Directiva no se hace mención a la coordinación, por la sencilla razón de que el SEPD no existía en el momento en que fue adoptada dicha Directiva, pero al cabo de seis años de existencia, el carácter complementario del SEPD y del Grupo de Trabajo es notorio y podría ser reconocido formalmente. El SEPD recuerda que en virtud del Reglamento (CE) nº 45/2001, tiene el deber de cooperar con las autoridades encargadas de la protección de datos y de participar en las actividades del Grupo de Trabajo. El SEPD recomienda mencionar explícitamente la cooperación en el nuevo instrumento jurídico y estructurarla cuando sea necesaria, por ejemplo, mediante el establecimiento de un procedimiento de cooperación.

10.6. *Cooperación entre el SEPD y las autoridades encargadas de la protección de datos en la supervisión de los sistemas de la Unión Europea*

156. Estas consideraciones se aplican también a los ámbitos en los que debe coordinarse la supervisión a nivel europeo y nacional. Tal es el caso de los organismos europeos que tratan cantidades significativas de datos enviados por las autoridades nacionales o los sistemas de información a gran escala con un componente europeo y un componente nacional.

157. El sistema existente para determinados organismos europeos y sistemas de información a gran escala — por ejemplo, Europol, Eurojust y el Sistema de Información de Schengen (SIS) de primera generación cuentan con autoridades comunes de control con representantes de las autoridades encargadas de la protección de datos — es un resto de la cooperación intergubernamental de la etapa anterior a Lisboa y no respeta la estructura institucional de la Unión Europea de la que ahora Europol y Eurojust son parte integrante y en la que se ha integrado el «acervo de Schengen» ([62]).

158. La Comunicación anuncia que la Comisión presentará en 2011 una consulta a las partes involucradas sobre la revisión de dichos sistemas de supervisión. El SEPD insta a la Comisión a que adopte una posición, tan pronto como sea posible, (dentro de un marco temporal breve y específico, véase más arriba) en el debate en curso sobre la supervisión. En este debate, se adoptará el punto de vista que se indica a continuación.

159. Como punto de partida, deberá garantizarse que todos los organismos de control cumplan los criterios indispensables de independencia, recursos y competencias coercitivas. Además, deberá garantizarse que se tengan en cuenta las perspectivas y la experiencia existentes a nivel europeo, lo que significa que la cooperación debería efectuarse no solo entre las autoridades nacionales sino también con la autoridad de protección de datos europea (actualmente el SEPD). El SEPD considera necesario seguir un modelo ajustado a estos requisitos ([63]).

160. En los últimos años, se ha desarrollado el modelo de «control coordinado». Dicho modelo de control, actualmente operativo en Eurodac y partes del Sistema de Información Aduanero, pronto se ampliará al Sistema de Información de Visados (VIS) y al Sistema de Información de Schengen de segunda generación (SIS II). El modelo

([61]) Por ejemplo sobre la base del inventario de actividades legislativas publicado anualmente y que se actualiza de manera regular, disponible en el sitio web del SEPD.

([62]) En virtud del Reglamento (CE) nº 45/2001, el SEPD tiene el deber de cooperar con estos organismos.

([63]) En el caso de Eurojust, debería tenerse en cuenta un control de la protección de datos que respete la independencia judicial, en relación con el tratamiento de datos de Eurojust en el ámbito de los procedimientos penales.

presenta tres aspectos: 1) la autoridad encargada de la protección de datos garantiza el control a escala nacional; 2) el SEPD garantiza el control a nivel europeo; 3) la coordinación se garantiza por medio de reuniones regulares acordadas por el SEPD, que actúa como secretario de este mecanismo de coordinación. El modelo se ha revelado eficaz y efectivo y debería contemplarse en el futuro para otros sistemas de información.

C. **¿CÓMO MEJORAR LA APLICACIÓN DEL PRESENTE MARCO?**

11. **A corto plazo**

161. Mientras esté en curso el proceso de revisión, deberán invertirse esfuerzos en garantizar la aplicación total y efectiva de las normas actuales. Dichas normas seguirán siendo aplicables hasta que se adopte el futuro marco y se incorpore a continuación a las legislaciones nacionales de los Estados miembros. En este sentido, se pueden apreciar varias líneas de actuación.

162. En primer lugar, la Comisión debe seguir velando por que los Estados miembros cumplan la Directiva 95/46/CE y, llegado el caso, utilicen sus facultades en virtud de lo dispuesto en el artículo 258 del TFEU. Recientemente, se han incoado procedimientos de infracción por aplicación incorrecta del artículo 28 de la Directiva en relación con el requisito de independencia de las autoridades encargadas de la protección de datos ([64]). Asimismo, en otros ámbitos deberá supervisarse y aplicarse el cumplimiento total ([65]). En consecuencia, el SEPD recibe con agrado y apoya plenamente el compromiso de la Comisión de proseguir una política activa de sanción de las infracciones. La Comisión debe continuar asimismo el diálogo estructural con los Estados miembros in relación con su aplicación ([66]).

163. En segundo lugar, debe alentar la aplicación a nivel nacional con el fin de garantizar una aplicación práctica de las normas de protección de datos, incluso en relación con los nuevos fenómenos tecnológicos y los operadores mundiales. Las autoridades encargadas de la protección de datos deberían hacer pleno uso de sus facultades de investigación y de sanción. También es importante que los derechos existentes de los interesados, en particular los derechos de acceso, se apliquen plenamente en la práctica.

164. En tercer lugar, parece necesaria a corto plazo una mayor coordinación en cuanto a la aplicación. A este respecto, resulta crucial la función del Grupo de Trabajo del artículo 29 y sus documentos interpretativos, aunque también las autoridades encargadas de la protección de datos deberán hacer todo lo posible para llevarlos a la práctica. Deben evitarse resultados divergentes en los casos europeos o mundiales y en el seno del Grupo de Trabajo pueden y deben alcanzarse enfoques comunes. Las investigaciones coordinadas a nivel europeo bajo los auspicios del Grupo de Trabajo también pueden aportar un significativo valor añadido.

165. En cuarto lugar, los principios relativos a la protección de datos deberán «integrarse» proactivamente en las nuevas disposiciones que puedan repercutir, directa o indirectamente, sobre la protección de datos. A nivel de la Unión Europea, el SEPD se esfuerza considerablemente en mejorar la legislación europea, esfuerzos que también deberán acometerse a escala nacional. Las autoridades encargadas de velar por la protección de datos deberán, por lo tanto, hacer pleno uso de sus facultades consultivas con el fin de garantizar un enfoque proactivo. Las autoridades encargadas de la protección de datos, incluido el SEPD, podrían jugar asimismo un papel proactivo en el control de la evolución tecnológica. La supervisión es importante para identificar en una fase inicial las nuevas tendencias, destacar posibles implicaciones para la protección de datos, apoyar soluciones respetuosas con la protección de datos y sensibilizar a las partes involucradas.

166. Por último, es necesario ahondar activamente en la cooperación entre los diversos actores a escala internacional. Es importante, pues, reforzar los instrumentos internacionales de cooperación. Iniciativas como las normas de Madrid y el trabajo en curso dentro del Consejo de Europa y la OCDE merecen pleno apoyo. En este contexto, resulta muy positivo que también se haya unido a la familia de las Autoridades de Protección de Datos y Protección de la Intimidad en el marco de la Conferencia Internacional, la Comisión Federal de Comercio de los Estados Unidos.

D. **CONCLUSIONES**

OBSERVACIONES DE CARÁCTER GENERAL

167. El SEPD acoge con agrado la Comunicación de la Comisión en general, ya que está convencido de que es necesario revisar el presente marco jurídico en materia de protección de datos, con el fin de garantizar una tutela efectiva en una sociedad de la información cada vez más desarrollada y globalizada.

168. La Comunicación identifica las cuestiones y retos principales. El SEPD comparte la opinión de la Comisión y piensa que en el futuro seguirá siendo necesario un sistema de protección de datos, basándose en la validez de los principios generales en vigor sobre protección de datos en una sociedad que experimenta cambios radicales. El SEPD comparte la declaración de la Comunicación en la que se afirma que los retos son enormes y subraya que las soluciones propuestas deben ser, por consiguiente, ambiciosas y contribuir a mejorar la eficacia de la protección. Por consiguiente, el SEPD pide un enfoque más ambicioso en relación con una serie de puntos.

169. El SEPD apoya plenamente el enfoque global en materia de protección de datos, si bien lamenta que la Comunicación excluya del instrumento jurídico general

([64]) Véase el asunto C-518/07, arriba mencionado y el Comunicado de Prensa de la Comisión de 28 de octubre de 2010 (IP/10/1430).

([65]) La Comisión ha incoado un procedimiento de infracción contra el Reino Unido por la supuesta violación de diversas disposiciones en materia de protección de datos, incluido el requisito de confidencialidad de las comunicaciones electrónicas en relación con la publicidad basada en el comportamiento. Véase el Comunicado de Prensa de la Comisión de 9 de abril de 2009 (IP/09/570).

([66]) Véase el primer informe de la Comisión sobre la aplicación de la Directiva sobre protección de datos mencionado anteriormente, p. 22 y ss.

determinados ámbitos, como el tratamiento de datos por parte de las instituciones y los organismos de la UE. Si la Comisión decidiera dejar fuera estos ámbitos, el SEPD insta a la Comisión a que adopte una propuesta a nivel europeo en el menor plazo posible, aunque preferentemente antes de la conclusión de 2011.

PRINCIPALES PERSPECTIVAS

170. En opinión del SEPD, los puntos de partida del proceso de revisión son los siguientes:

— las disposiciones relativas a la protección de datos deben ofrecer, en la medida de lo posible, un apoyo activo en lugar de obstaculizar otros intereses legítimos (como la economía europea, la seguridad de las personas y la responsabilidad de los gobiernos);

— los principios generales de la protección de datos no pueden ni deben ser modificados;

— uno de los objetivos clave de la revisión debe ser una mayor armonización;

— el proceso de revisión debe afrontarse desde la perspectiva de los derechos fundamentales; los derechos fundamentales tienen como fin proteger a los ciudadanos en todas las circunstancias;

— el nuevo instrumento jurídico deberá incluir al sector policial y judicial;

— el nuevo instrumento jurídico debe formularse, en la medida de lo posible, de un modo neutro desde el punto de vista tecnológico y su objetivo debe consistir en generar seguridad jurídica a largo plazo.

ELEMENTOS DEL NUEVO MARCO

Armonización y simplificación

171. El SEPD recibe con agrado el compromiso de la Comisión de examinar los medios para lograr una mayor armonización de la protección de datos a nivel de la Unión. El SEPD determina ámbitos en los que es urgente una mayor y mejor armonización: las definiciones, los motivos (esto es, la base legal) para el tratamiento de datos, los derechos de los interesados, las transferencias internacionales y las autoridades de protección de datos.

172. El SEPD sugiere que se tengan en cuenta las siguientes alternativas para simplificar o reducir el ámbito de aplicación de los requisitos de notificación:

— limitar la obligación de notificación a determinados tipos de operaciones de tratamiento que impliquen riesgos específicos;

— establecer una simple obligación de registro que obligue a que sean los responsables del tratamiento de datos quienes realicen dicho registro (en oposición con el registro exhaustivo de todas las operaciones de tratamiento de datos);

— introducir un formulario de notificación estándar paneuropeo.

173. Según el SEPD un reglamento, único instrumento directamente aplicable en los Estados miembros, es el medio más eficaz para proteger el derecho fundamental a la protección de datos y para lograr una mayor convergencia en el mercado interior.

Reforzar los derechos de las personas

174. El SEPD apoya la propuesta de la Comunicación de reforzar los derechos de las personas y formula las siguientes sugerencias:

— debería incluirse un principio de transparencia en la legislación. Sin embargo, resulta más importante reforzar las disposiciones existentes que abordan la transparencia (como los existentes artículos 10 y 11 de la Directiva 95/46/CE).

— debería introducirse en el instrumento general, una disposición sobre la notificación de las violaciones de datos personales, que amplía la obligación incluida en la Directiva 2002/58, que fue objecto de revisión en 2011 a todos los responsables del tratamiento de datos;

— debería aclararse los límites del consentimiento; debería considerarse la ampliación de los casos en los que se exige un consentimiento expreso, así como la adopción de normas complementarias para el entorno en línea;

— deberían introducirse otros derechos como la portabilidad de los datos y el derecho al olvido, especialmente para los servicios de la sociedad de la información en Internet;

— deberían protegerse mejor los intereses de los niños mediante una serie de disposiciones adicionales, específicamente destinadas a la obtención y posterior tratamiento de los datos de los niños;

— deberían introducirse en la legislación europea, mecanismos de recurso colectivo para las violaciones de protección de datos, con el fin de habilitar a las entidades cualificadas a presentar demandas en representación de grupo de personas.

Reforzar el papel de las organizaciones/responsables del tratamiento

175. El nuevo marco debe incluir incentivos para que los responsables del tratamiento incluyan de manera proactiva medidas de protección de los datos en sus procesos empresariales. El SEPD propone la introducción de una obligación general sobre la responsabilidad y la intimidad mediante el diseño. Debería asimismo introducirse una disposición sobre los regímenes de certificación de la privacidad.

Globalización y Derecho aplicable

176. El SEPD apoya la ambiciosa labor de desarrollo de las llamadas «normas de Madrid» en el marco de la Conferencia Internacional de Autoridades de Protección de Datos, con el fin de integrarlas en un instrumento vinculante y posiblemente iniciar una conferencia intergubernamental. El SEPD pide a la Comisión que adopte pasos concretos en este sentido, en estrecha colaboración con la OCDE y el Consejo de Europa.

177. El nuevo instrumento jurídico debe aclarar los criterios de determinación de la legislación aplicable. Debería garantizarse que los datos que se tratan fuera de las fronteras de la Unión Europa no escapan de la jurisdicción de la Unión cuando exista un motivo justificado para aplicar la legislación europea. Si el marco jurídico tuviera la forma de un reglamento existirían normas idénticas en todos los Estados miembros y sería menos relevante determinar la legislación aplicable (dentro de la Unión).

178. El SEPD apoya totalmente el objetivo de garantizar un enfoque uniforme y coherente en relación con los terceros países y las organizaciones internacionales. En el instrumento jurídico, deben incluirse normas vinculantes para las empresas.

Ámbito policial y judicial

179. Un instrumento global que incluya el ámbito policial y judicial permite normas especiales que tienen debidamente en cuenta las especificidades de este sector, con arreglo a la Declaración 21 anexa al Tratado de Lisboa. Deben aplicarse salvaguardias específicas para compensar al interesado, concediéndole una protección complementaria en un ámbito en que el tratamiento de datos personales puede ser más invasivo de la intimidad.

180. El nuevo marco jurídico debe ser, en la medida de lo posible, claro, simple y coherente. Debe evitarse la proliferación de diferentes regímenes que se aplican, por ejemplo, a Europol, Eurojust, a los sistemas SIS y de la Declaración Prüm. El SEPD entiende que la tarea de alinear las normas de los distintos sistemas debe llevarse a cabo de manera cuidadosa y gradual.

Autoridades encargadas de la protección de datos y la cooperación entre ellas

181. El SEPD apoya totalmente el objetivo de la Comisión de tratar la cuestión del estatuto de las autoridades encargadas de la protección de datos y de reforzar su independencia, recursos y competencias coercitivas. El SEPD recomienda:

— codificar en el nuevo instrumento jurídico el concepto esencial de independencia de las autoridades encargadas de la protección de datos, tal como especifica el Tribunal de Justicia Europeo;

— establecer legalmente que debe dotarse de recursos suficientes a las autoridades encargadas de la protección de datos;

— proporcionar a las autoridades facultades sancionadoras y de investigación armonizadas.

182. El SEPD sugiere otras mejoras del funcionamiento del Grupo de Trabajo del artículo 29, incluidas aquellas relacionadas con su infraestructura e independencia. Debería proporcionarse asimismo al Grupo de Trabajo los recursos suficientes y una secretaría reforzada.

183. El SEPD sugiere reforzar el papel consultivo del Grupo de Trabajo mediante la introducción de la obligación, para las autoridades encargadas de la protección de datos y la Comisión, de *tener plenamente en cuenta los dictámenes y posiciones comunes* adoptadas por el Grupo de Trabajo. El SEPD no está a favor de dotar de fuerza vinculante a las posiciones del Grupo de Trabajo, en especial dado el carácter independiente de las autoridades encargadas de la protección de datos. El SEPD recomienda que la Comisión introduzca en el nuevo instrumento jurídico disposiciones específicas para aumentar la cooperación con el SEPD.

184. El SEPD insta a la Comisión a que adopte una posición, tan pronto como sea posible, sobre la cuestión del control de los organismos de la Unión y los sistemas de información a gran escala, teniendo en cuenta que todos los organismos de control deberían cumplir los criterios indispensables de independencia, recursos suficientes y competencias coercitivas, y que debería garantizarse que la perspectiva de la Unión está bien representada. El SEPD apoya el modelo de «control coordinado».

Mejoras con arreglo al sistema actual:

185. El SEPD anima a la Comisión a que:

— siga controlando que los Estados miembros cumplen la Directiva 95/46/CE y, cuando sea necesario, utilice sus competencias coercitivas con arreglo a lo dispuesto en el artículo 258 del TFEU;

— promueva la aplicación a nivel nacional y la coordinación de la aplicación;

— integre los principios de protección de datos de manera proactiva en las nuevas normativa que pueden tener un impacto, directo o indirecto, sobre la protección de datos;

— persiga activamente una mayor cooperación entre los diversos operadores a nivel internacional.

Hecho en Bruselas, el 14 de enero de 2011.

Peter HUSTINX

Supervisor Europeo de Protección de Datos