DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos relativo a la Decisión 2011/141/UE de la Comisión que modifica la Decisión 2007/76/CE de la Comisión sobre el Sistema de Cooperación para la Protección de los Consumidores (CPCS) y sobre la Recomendación 2011/136/UE de la Comisión sobre las directrices para la aplicación de las normas de protección de datos en el CPCS

(2011/C 217/06)

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],

vista la solicitud de dictamen, hecha de conformidad con el artículo 28, apartado 2, del 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 y a la libre circulación de estos datos [2];

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. INTRODUCCIÓN

1. El 1 de marzo de 2011, la Comisión Europea adoptó una decisión de la Comisión que modifica la Decisión 2007/76/CE de la Comisión relativa al CPCS («segunda modificación de la CPC») [3]. Ese mismo día, la Comisión también adoptó la Recomendación de la Comisión sobre directrices para la aplicación de las normas de protección de datos en el Sistema de Cooperación para la Protección del Consumidor (CPCS) (en lo sucesivo, las «directrices de protección de datos de la CPC») [4]. Ambos documentos se trasladaron para consulta al SEPD de conformidad con lo dispuesto en el artículo 28, apartado 2, del Reglamento (CE) nº 45/2001.

2. El CPCS es un sistema tecnológico de información diseñado y gestionado por la Comisión de conformidad con lo dispuesto en el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores (en lo sucesivo, el «Reglamento CPC»). El sistema CPCS facilita la cooperación entre las «autoridades competentes» de los Estados miembros y la Comisión en el ámbito de la protección de los consumidores, respecto a las infracciones de un conjunto predefinido de directivas y reglamentos europeos. Para que dichas infracciones entren dentro del ámbito de aplicación del Reglamento CPC, éstas deben tener un carácter transfronterizo y deben perjudicar los «intereses colectivos de los consumidores».

3. En el marco de su cooperación, los usuarios del CPCS intercambian información, incluidos datos personales. Dichos datos personales pueden estar relacionados con los directores o empleados de un comerciante o proveedor presunto infractor, con el propio comerciante o proveedor (si se trata de una persona física), así como con terceros como los consumidores o denunciantes.

4. El sistema está diseñado para funcionar como una herramienta de comunicación segura entre las autoridades competentes así como una base de datos. Las autoridades competentes utilizan el sistema CPCS para solicitar información que les ayude a investigar un caso [5] o solicitar asistencia para la aplicación [6] («solicitudes de asistencia mutua»). Además, las autoridades competentes también podrán enviar mensajes de alerta («alertas»), para informar a otras autoridades competentes y a la Comisión sobre una infracción o una sospecha de infracción [7]. El CPCS contiene asimismo otras funcionalidades, incluido un sistema de

[1] DO L 281 de 23.11.1995, p. 31.
[2] DO L 8 de 12.1.2001, p. 1.
[3] Decisión de la Comisión de 1 de marzo de 2011 que modifica la Decisión 2007/76/CE, por la que se aplica el Reglamento (CE) nº 2006/2004 del Parlamento Europeo y del Consejo, sobre la cooperación entre las autoridades nacionales encargadas de la aplicación de la legislación de protección de los consumidores, en lo que respecta a la asistencia mutua (2011/141/UE) (DO L 59 de 4.3.2011, p. 63).
[4] Recomendación de la Comisión de 1 de marzo de 2011 sobre directrices para la aplicación de las normas de protección de datos en el Sistema de Cooperación para la Protección del Consumidor (CPCS); (2011/136/UE) (DO L 57 de 2.3.2011, p. 44).
[5] Véase el artículo 6 del Reglamento CPC sobre el «intercambio de información previa solicitud».
[6] Véase el artículo 8 del Reglamento CPC sobre las «solicitudes de medidas de aplicación».
[7] Véase el artículo 7 del Reglamento CPC sobre el «intercambio de información sin solicitud previa».

notificación ([8]) y un foro para intercambiar datos no vinculados con los casos.

5. En el presente dictamen, el SEPD trata una serie de cuestiones en materia de protección de datos relativas al marco jurídico del sistema CPCS, centrándose principalmente en la recientemente adoptada segunda modificación de la CPC. Por otro lado, el SEPD hace balance de los avances logrados hasta la fecha y destaca de manera selectiva algunas preocupaciones que subsisten y consideraciones para el futuro. Asimismo, también realiza observaciones sobre algunas disposiciones de las directrices de protección de datos de la CPC.

6. De manera paralela al presente dictamen (que se adopta de conformidad con lo dispuesto en el artículo 28, apartado 2, del Reglamento (CE) nº 45/2001), el SEPD también emite un dictamen de control previo, en el ejercicio de sus competencias de supervisión (con arreglo a lo dispuesto en el artículo 27 de dicho Reglamento) (en lo sucesivo, el «dictamen de control previo»). El dictamen de control previo incluye una descripción más detallada del sistema CPCS, así como de los tratamientos de datos personales dentro del mismo. En dicho dictamen, el SEPD se centra en recomendar que se adopten medidas en el plano práctico, técnico y organizativo a fin de mejorar el cumplimiento de las normas de protección de datos en el CPCS. Teniendo en cuenta que las directrices de protección de datos de la CPC también guardan una estrecha relación con dichas medidas específicas, el dictamen de control previo realiza asimismo observaciones sobre las disposiciones seleccionadas de las directrices.

II. MARCO JURÍDICO DEL CPCS

7. Al SEPD le complace que el CPCS tenga un fundamento jurídico sólido, en particular, un reglamento adoptado por el Consejo y el Parlamento. Asimismo, al SEPD le satisface que el fundamento jurídico se haya complementado con el paso del tiempo para incluir más detalles y tratar cuestiones relativas a la protección de datos. En particular, al SEPD le complace que se adoptara la Decisión 2007/76/CE de la Comisión, de 22 de diciembre de 2006, por la que se aplica el Reglamento CPC (en lo sucesivo, la «Decisión de aplicación del Reglamento CPC»), la cual fue modificada posteriormente el 17 de marzo de 2008 y, más recientemente, el 1 de marzo de 2011, mediante la segunda modificación de la CPC. También se congratula de que la Comisión adoptara las directrices de protección de datos de la CPC, que tratan de manera específica cuestiones relativas a la protección de datos.

8. Aunque el SEPD lamenta no haber sido consultado en el momento en que se adoptaron inicialmente el Reglamento CPC y la Decisión de aplicación del Reglamento CPC, está satisfecho de que la Comisión le consultara en el momento de adoptar tanto las dos modificaciones de la Decisión de aplicación del Reglamento CPC como las directrices de protección de datos de la CPC. El SEPD está asimismo satisfecho de que la Comisión también consultara previamente al Grupo de Trabajo sobre protección de datos del artículo 29 (en lo sucesivo, el «GT29»), quien emitió, a fecha de 21 de septiembre de 2007, su Dictamen nº 6/2007 (WP 139). Por último, el SEPD recibe con agrado el hecho de que se hayan hecho referencias a estas consultas en el preámbulo de las directrices de protección de datos CPC.

9. El SEPD destaca: (i) que la Comisión ha considerado detenidamente las recomendaciones del SEPD, proporcionadas en intercambios informales previos, así como la opinión expresada por el GT29 en su Dictamen nº 6/2007; y que (ii) se hayan seguido muchas de estas recomendaciones a la hora de desarrollar un marco legislativo para el CPCS y/o en el plano práctico, técnico y organizativo. Las observaciones incluidas en el presente dictamen, así como en el dictamen de control previo, deben considerarse en este contexto positivo.

III. CUESTIONES EN MATERIA DE PROTECCIÓN DE DATOS RESPECTO DE LA SEGUNDA MODIFICACIÓN DE LA CPC

3.1. Conservación de datos personales en el CPCS

3.1.1. *Introducción*

10. Como observación preliminar, el SEPD señala que el Reglamento CPC no ha tratado de manera adecuada y global la cuestión de los cierres de los casos y los períodos de conservación ([9]).

11. De hecho, el Reglamento CPC únicamente establece dos normas específicas relativas a la supresión de los datos y ninguna en relación con el cierre de casos ([10]). En primer lugar, establece que cuando una alerta «se revele infundada», la autoridad competente deberá retirarla y la Comisión deberá suprimir inmediatamente la información de la base de datos. En segundo lugar, exige que cuando una autoridad competente notifica, en virtud de lo dispuesto en el artículo 8, apartado 6, del Reglamento CPC, que la infracción ha cesado, los datos almacenados deberán borrarse a los cinco años de la notificación.

12. El Reglamento CPC no establece la finalidad del período de conservación de cinco años, ni establece más especificaciones sobre el modo y el momento en que debe considerarse que una alerta es «infundada». Asimismo, el Reglamento CPC también guarda silencio en relación con el período en que la información debe conservarse en la base de datos en los casos que no queden cubiertos por las dos normas

([8]) Véase el artículo 7, apartado 2, y el artículo 8, apartado 6, del Reglamento CPC.

([9]) Véase también el Dictamen nº 6/2007 del Grupo de Trabajo sobre protección de datos del artículo 29 (mencionado en el apartado II).

([10]) Véase el artículo 10, apartado 2, del Reglamento CPC.

específicas citadas anteriormente (por ejemplo, el Reglamento no especifica el tiempo en que deben conservarse las solicitudes de asistencia mutua en la base de datos, si éstas no han conducido a una acción de aplicación adecuada que haya cesado la infracción).

13. El SEPD recibe con satisfacción que la Decisión de aplicación del Reglamento CPC, modificada, y que las directrices de protección de datos de la CPC intenten ofrecer algunas aclaraciones. Precisado lo anterior, el SEPD sigue preocupado por diversos aspectos relativos a las normas de cierre de casos y de conservación de datos en el CPCS, tal como se ha indicado en los apartados 3.1.2 a 3.1.4.

14. El SEPD recomienda que en la próxima revisión del marco jurídico del CPCS se traten estas preocupaciones, a través de la modificación de la Decisión de aplicación del Reglamento CPC o, preferentemente, a través de la modificación del propio Reglamento CPC.

15. Hasta que dicha acción legislativa sea posible, el SEPD recomienda que las preocupaciones relativas a los períodos de conservación se traten desde un plano práctico, técnico y organizativo y se establezcan de manera clara en el documento «La red de cooperación en materia de protección de los consumidores: Directrices operativas» mencionado en el apartado 3.1.2 *infra*.

3.1.2. *Oportuno cierre de casos*

16. La segunda modificación de la CPC no establece una fecha final en la que deben cerrarse los casos que impliquen una solicitud de asistencia mutua (solicitud de información o solicitud de aplicación).

17. En el dictamen de control previo, el SEPD toma nota de una serie de medidas prácticas que la Comisión está adoptando para contribuir a garantizar que los casos dormidos se cierran de manera oportuna.

18. En el presente dictamen, el SEPD recomienda que se establezcan plazos máximos para las solicitudes de información y para las solicitudes de aplicación, lo cual debería quedar especificado en el marco legislativo en la próxima revisión. Los plazos deben estar relacionados con el tipo de caso, así como con la actividad real. Al mismo tiempo, las normas deberían ofrecer flexibilidad a las autoridades competentes para que éstas pudieran ampliar el caso por un buen motivo, a fin de garantizar que los casos no se cierran de manera prematura, incluso si, de este modo, un caso complejo supera el plazo medio de cierre.

19. Para ello, el SEPD recomienda emplear como punto de partida el documento titulado «La red de cooperación en materia de protección de los consumidores: Directrices operativas» aprobado por el Comité CPC el 6 de diciembre de 2010. Las Directrices operativas, en el punto 2.7, bajo el título «fases y plazos de un caso CPC», trata sobre los flujos de los casos típicos y establece que las solicitudes de información deben gestionarse, como media, en un plazo de uno a tres meses. El tratamiento de las solicitudes de aplicación, según las directrices operativas, deberá ser factible en el plazo medio de seis a nueve meses (salvo en caso de acciones de cesación o en caso de que se interponga un recurso contra una decisión administrativa, en los cuales es más realista que el plazo sea de un año o más).

3.1.3. *Alertas*

20. La segunda modificación de la CPC introduce un nuevo apartado en el punto 2.2.2 del Anexo a la Decisión de aplicación del Reglamento CPC el cual exige que las alertas «fundadas» deben ser eliminadas de la base de datos cinco años después de su emisión (respecto de las alertas «infundadas», las disposiciones existentes todavía requieren su supresión una vez que «la alerta se revele infundada»).

21. Para poner esta nueva disposición en su contexto, el SEPD destaca que una de las principales preocupaciones es garantizar que los datos personales no se mantienen en la base de datos CPC durante más tiempo del que resulte necesario. Esta es una cuestión delicada en especial en relación con las alertas (que tienen un número mayor de destinatarios que los intercambios bilaterales) y, entre ellas, en especial en relación con aquellas que se refieren a supuestas infracciones. En la práctica, la falta de un plazo claro de conservación de una alerta abierta implicaría que algunas alertas podrían quedar pendientes indebidamente durante un largo período (durante el tiempo en que no se revele claramente que está infundada). Dichas acciones basadas en sospechas no confirmadas entrañarían significativos riesgos para el derecho fundamental de protección de datos, así como para otros derechos fundamentales como el de presunción de inocencia.

22. En este contexto, al SEPD le complace que se haya establecido un período de conservación para las alertas. Sin embargo, el SEPD considera que la Comisión no ha proporcionado una justificación adecuada que demuestre que un período de conservación de cinco años resulte proporcionado. El SEPD recomienda a la Comisión que realice una valoración de la proporcionalidad y evalúe de nuevo la extensión del período de conservación para las alertas. En principio, todas las alertas sobre las que se informe deberán ser suprimidas de la base de datos mucho antes, salvo si se trata de una alerta sobre una infracción o una sospecha de infracción que ha generado una solicitud de asistencia mutua y la investigación transfronteriza o la acción de aplicación todavía está en curso. El período de conservación debería ser lo suficientemente largo para permitir a cada una de las autoridades que reciben el mensaje establecer si desea adoptar pasos de investigación o acciones de aplicación, y si desea enviar una solicitud de asistencia mutua a través del CPCS. Sin embargo, debería ser lo suficientemente corto para minimizar los riesgos de que las alertas puedan ser utilizadas de forma indebida para elaborar listas negras o extraer datos.

23. Desde esta perspectiva, el SEPD recomienda que la Comisión revise el marco jurídico para garantizar que las alertas se suprimen como máximo en los seis meses siguientes a su introducción, salvo que pueda justificarse un período de conservación más adecuado.

24. Lo anterior debería ayudar a garantizar, en particular, que en los casos en que la sospecha no se haya confirmado (o que ni siquiera se haya investigado), las personas físicas que sean inocentes que se vinculen a la sospecha no se mantengan en la «lista negra» o «bajo sospecha» durante un período indebidamente largo, lo cual no sería conforme a lo dispuesto en el artículo 6, letra e), de la Directiva 95/46/CE.

25. Esta limitación resulta asimismo necesaria para garantizar el principio de calidad de los datos (véase el artículo 6, letra d), de la Directiva 95/46/CE) así como otros principios jurídicos importantes. Lo anterior no solo daría lugar a un nivel de protección más adecuado para las personas físicas, sino que también permitiría, al mismo tiempo, que los funcionarios encargados de hacer cumplir la legislación se centrasen de manera más eficaz en los casos importantes.

3.1.4. *Período de conservación de las solicitudes de asistencia mutua cerradas*

26. La segunda modificación de la CPC añadió un nuevo párrafo al punto 2.15 del anexo de la Decisión de aplicación del Reglamento CPC para exigir que «[c]ualquier otra información relacionada con solicitudes de asistencia mutua con arreglo al artículo 6 del (Reglamento CPC) se eliminará de la base de datos cinco años después de cerrarse el asunto.».

27. Junto con el texto existente, el punto 2.15 revisado exige una conservación de cinco años de todos los intercambios de información después de que se haya cerrado el asunto, con arreglo al artículo 6, salvo:

— si se han suprimido datos erróneos,

— si el intercambio de información no ha generado una alerta o una solicitud de aplicación, o

— si se ha establecido que no se cometió ninguna infracción en el sentido del Reglamento CPC.

28. De hecho, tal como se explicó en el dictamen de control previo, el tiempo de conservación «estándar» aplicado en el CPCS después del cierre de casos (sujeto a excepciones específicas) es de cinco años tanto para las solicitudes de información como para las solicitudes de aplicación.

29. El texto de la Decisión de aplicación del Reglamento CPC modificado por la segunda modificación de la CPC no parece plenamente compatible con el Reglamento CPC. En particular, el artículo 10, apartado 2, del Reglamento CPC distingue, por un lado, entre la información intercambiada que resulta en una aplicación efectiva (es decir, los casos en que la infracción ha cesado a resultas de las acciones de aplicación que se han adoptado) y, por otro lado, la información que no ha resultado en una aplicación efectiva. En el primer caso, se prevé un período de conservación de cinco años desde que se ha cerrado el caso. En el segundo caso, no se han establecido disposiciones específicas (salvo para las alertas infundadas que deben ser retiradas y suprimidas).

30. Dicho de otro modo, el Reglamento CPC exige un período de conservación de cinco años después del cierre de un caso únicamente si se han adoptado acciones de aplicación y éstas han logrado cesar la infracción.

31. Aunque el SEPD tiene dudas respecto de la finalidad y la proporcionalidad de la conservación de cualquier dato durante cinco años hasta que el asunto se cierre (véanse las observaciones incluidas en el apartado 3.1.4), distinguir entre los casos que han acabado en una medida de aplicación y los que no, no parece tener ninguna lógica desde el punto de vista de la protección de datos. En particular, la conservación de datos relativa a las meras sospechas durante un período largo tiene una mayor probabilidad de ser imprecisa y también está expuesta al riesgo de infringir otros principios jurídicos importantes. Por tanto, puede decirse que, en general, es más probable que la conservación de dichos datos durante un largo período plantee más problemas en materia de protección de datos que la conservación de datos relativa a infracciones reales, que se han probado de manera adecuada y han derivado en una acción de aplicación.

32. Contrario a lo dispuesto en el Reglamento CPC, la Decisión de aplicación del Reglamento CPC modificada parece permitir, al menos en algunos casos, que el período de conservación de cinco años también se aplique a la información que no conduce a la adopción de acciones de aplicación.

33. Por ejemplo, según la Decisión de aplicación del Reglamento CPC, una solicitud de información que derive en una alerta pero que no lleve a una acción de aplicación parece quedar en el sistema durante cinco años después de cerrarse el asunto.

34. El Reglamento CPC y la Decisión de aplicación del Reglamento CPC parece que siguen enfoques algo distintos. La Decisión de aplicación del Reglamento CPC, aunque refleja en cierta medida las disposiciones del Reglamento CPC, también introduce otras normas importantes para la conservación. Aunque sería bien recibida una aclaración de las normas, el SEPD cuestiona la legitimidad de establecer períodos de conservación más largos a los que ya exigía el Reglamento CPC, lo cual impondría mayores restricciones tanto al derecho fundamental de protección de datos como a la legislación de aplicación, contrarias al Reglamento CPC y a la normativa en materia de protección de datos aplicable.

35. De conformidad con lo anterior, el SEPD recomienda a la Comisión que revise el marco jurídico y reconsidere si el período de conservación de cinco años debería aplicarse a cualquier otro caso distinto de los de aquellos en que han sido adoptadas acciones de aplicación, con arreglo a lo dispuesto en el Reglamento CPC.

36. Además, al SEPD le complace que las directrices de protección de datos de la CPC tengan por objeto especificar el fin de la conservación después del cierre del caso, cuestión ésta importante que no es tratada ni en el Reglamento CPC ni en la segunda modificación de la CPC. En particular, las directrices de protección de datos CPC establecen que «durante el período de conservación, los funcionarios autorizados encargados de hacer cumplir la legislación que trabajen para una autoridad competente que ha tratado originalmente un caso pueden consultar el expediente para establecer vínculos con infracciones posiblemente repetidas, a fin de contribuir a un cumplimiento mejor y más eficaz.» ([11]).

37. Sin embargo, aunque se recibe con agrado esta aclaración, a falta de una mayor justificación de la necesidad de dicho acceso, el SEPD no está convencido que este fin resulte proporcional y suficiente para justificar un período de conservación de cinco años. Por tanto, el SEPD recomienda a la Comisión:

— aclarar con más detalle el fin del período de conservación de cinco años;

— evaluar si un período de conservación más corto permitiría lograr los mismos objetivos; y

— evaluar si toda la información prevista actualmente requiere ser conservada o si bastaría con un subconjunto de dicha información (por ejemplo, debe considerarse si sería suficiente únicamente conservar las notificaciones previstas en el artículo 8, apartado 6; debería evaluarse específicamente si la conservación de los nombres de los directores o de los anexos puede incluir otros datos personales distintos de los necesarios; debería hacerse también una distinción entre los datos relativos a las supuestas infracciones y a las infracciones «probadas»).

3.2. **Acceso de la Comisión a los datos en el CPCS**

38. El SEPD recibe con agrado que (al introducir un nuevo punto 4.3 al anexo de la Decisión de aplicación del Reglamento CPC), la segunda modificación de la CPC aclare el acceso de la Comisión a los datos en el CPCS y que dicho acceso esté clara y específicamente limitado a lo requerido con arreglo al Reglamento CPC. En particular, al SEPD le complace que a la Comisión no se le haya dado acceso a las comunicaciones confidenciales entre las autoridades competentes de los Estados miembros, como las solicitudes de asistencia mutua.

39. Tanto la aclaración como la limitación son especialmente importantes, teniendo en cuenta que la falta de claridad podría llevar a una situación en que la Comisión pudiera tener acceso a la información, incluidos datos personales, que está únicamente destinada a las autoridades competentes de los Estados miembros.

40. Tal como se describe en el apartado 5 de las Directrices de protección de datos de la CPC, «el objetivo del acceso de la Comisión es supervisar la aplicación del Reglamento CPC y de la legislación de protección de los consumidores que figura en el anexo del Reglamento CPC, así como compilar información estadística relacionada con la realización de dichas tareas.».

41. Esto no significa que la Comisión deba tener acceso a cualquiera de los datos intercambiados entre los Estados miembros en el CPCS.

42. De hecho, el SEPD destaca que el acceso a bases de datos como el CPCS entra dentro de la definición del tratamiento de datos personales. De acuerdo con lo dispuesto en el artículo 5, letra a), del Reglamento (CE) nº 45/2001, que resulta pertinente para los derechos de acceso de la Comisión en el CPCS, las instituciones sólo podrán efectuar el tratamiento de datos personales si esto es necesario para el cumplimiento de una misión de interés público y siempre que el tratamiento esté basado en los Tratados o en la legislación secundaria.

([11]) Véase la sección 8 de las Directrices, «Directrices adicionales; ¿Por qué el período de conservación es de cinco años?» Las Directrices de protección de datos CPC añaden asimismo que «el propósito del período de conservación es facilitar la cooperación entre las autoridades públicas encargadas de hacer cumplir la legislación protectora de los intereses de los consumidores durante el examen de las infracciones intracomunitarias, así como contribuir al buen funcionamiento del mercado interior, a la calidad y coherencia del cumplimiento de la legislación protectora de los intereses de los consumidores, al control de la protección de los intereses económicos de estos y a elevar los niveles y la coherencia del cumplimiento de la legislación.».

43. El SEPD entiende que estos requisitos – que derivan directamente del derecho a la protección de datos consagrado en el artículo 8 del Convenio Europeo de Derechos Humanos y en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea – implican que la Comisión únicamente tendrá poder para acceder a los sistemas de información de los Estados miembros si así está establecido en las disposiciones jurídicas específicas, sobre la base de un fundamento jurídico adecuado (normalmente el procedimiento legislativo ordinario). La seguridad jurídica y la transparencia son dos valores subyacentes que explican el motivo por el que un fundamento específico y una base jurídica segura para el acceso de la Comisión resulta una garantía especialmente importante para asegurar los derechos fundamentales de las personas respecto de la protección de datos.

44. Ni el poder de vigilancia general de la Comisión como «guardiana de los Tratados» ni la obligación de los Estados miembros de garantizar una cooperación leal resultan lo suficientemente precisos para permitir el acceso de la Comisión a las bases de datos que contengan datos personales. La cooperación leal implica que los Estados miembros deberían – en determinadas condiciones – proporcionar información a la Comisión cuando así les sea solicitado o cuando dicha información se les exija con arreglo a lo dispuesto en una norma específica. Sin embargo, no implica que la Comisión deba tener acceso a sus bases de datos.

45. En este contexto, el SEPD destaca asimismo que el Reglamento CPC excluye la posibilidad de acceso por parte de la Comisión a la información contenida en las solicitudes de asistencia mutua y de aplicación. Los artículos 6 y 8 del Reglamento CPC designan únicamente a las autoridades solicitantes, y no a la Comisión, como destinatarias de dichos datos.

3.3. **Categorías especiales de datos en el CPCS**

46. Al SEPD le complace que la segunda modificación de la CPC haya introducido, en el punto 4.4 del anexo de la Decisión de aplicación del Reglamento CPC, una disposición que aborda el tratamiento de categorías especiales de datos en el CPCS. El SEPD recibe con especial agrado que la disposición limite dicho tratamiento a los casos en que el cumplimiento de las obligaciones establecidas en el Reglamento CPC sea «de otro modo imposible» y que el tratamiento de estos datos quede sujeto a la condición adicional de que esté «permitido conforme a la Directiva 95/46/CE».

IV. **INTIMIDAD MEDIANTE EL DISEÑO Y RENDICIÓN DE CUENTAS**

47. Después de analizar en el apartado III las cuestiones específicas planteadas por la segunda modificación de la CPC, en los apartados IV a VI, el SEPD desea llamar la atención de la Comisión hacia algunos puntos que deberían ser considerados para el futuro desarrollo del marco jurídico del CPCS.

4.1. **Intimidad mediante el diseño**

48. Durante algún tiempo, el SEPD ha animado a la Comisión y a otras instituciones europeas a que adopten medidas técnicas y organizativas que integren la protección de datos y la seguridad como una parte fundamental del diseño y de la aplicación de sus sistemas de información («intimidad mediante el diseño») ([12]).

49. A pesar de recibir con agrado y reconocer que se han adoptado algunas medidas en este sentido, el SEPD recomienda a la Comisión que realice una evaluación global sobre las garantías de la intimidad mediante el diseño que podrían incorporarse en la arquitectura del sistema CPCS. Entre otros, deberían considerarse y aplicarse las siguientes acciones:

— soluciones de intimidad mediante el diseño para guiar a los usuarios del sistema a adoptar decisiones «adecuadas» en materia de protección de datos (véase el apartado 3.2 del dictamen de control previo);

— medidas para facilitar el oportuno cierre y supresión de los asuntos (*ídem*, apartado 3.3);

— procedimientos para facilitar información y el acceso a los derechos a los interesados (*ídem*, apartado 3.5);

— procedimientos claros para cualquier modificación realizada directamente en el plano de la base de datos, el acceso de conexión, el racional de la acción y la aprobación, en el plano de la adecuación (*ídem*, apartado 3.6); y

— almacenamiento «encriptado» de la información en la base de datos de modo que los operadores tecnológicos no puedan acceder a la misma (al menos para algunos datos como los anexos confidenciales) (*ídem*, apartado 3.6).

4.2. **Rendición de cuentas**

50. Además, de conformidad con el principio de «rendición de cuentas» ([13]), el SEPD recomienda asimismo establecer un marco claro de rendición de cuentas que garantice el cumplimiento en materia de protección de datos y aporte pruebas de ello, como:

([12]) Véase el apartado 7 del Dictamen del SEPD 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», emitido el 14 de enero de 2011 (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf)

([13]) Ídem.

— la adopción y la actualización, cuando sea necesario, de una política de protección de datos que debe aprobarse al más alto nivel de gestión en la DG SANCO. Dicha política de protección de datos deberá también incluir un plan de seguridad (véase el apartado 3.6 del dictamen de control previo) ([14]);

— la realización de auditorías periódicas para valorar la adecuación y el cumplimiento continuado de la política de protección de datos (incluida la auditoría del plan de seguridad, ídem, apartado 3.6);

— la publicación (al menos parcialmente) de los resultados de dichas auditorías para garantizar a las partes interesadas el cumplimiento de la legislación sobre protección de datos; y

— la notificación de las violaciones de datos y otros incidentes de seguridad a la Comisión DPO, a los interesados afectados (y otras partes interesadas y autoridades, en su caso) ([15]).

V. TRANSMISIÓN DE DATOS PERSONALES FUERA DE LA UNIÓN EUROPEA

5.1. Acuerdos bilaterales

51. El artículo 14, apartado 2, del Reglamento CPC establece que una autoridad competente podrá también transmitir a la autoridad de un tercer país información con arreglo al Reglamento CPC en el marco de un acuerdo bilateral de asistencia mutua con dicho país siempre que (i) la autoridad competente que envió inicialmente la información dé su consentimiento y que (ii) la transmisión sea conforme con la legislación comunitaria en materia de protección de datos aplicable.

52. Los artículos 25 y 26 de la Directiva 95/46/CE sujetan las transmisiones a terceros países a determinadas condiciones adicionales. Estas condiciones tienen por objeto garantizar que los datos se protegerán de manera adecuada en el extranjero. Además, también establecen una serie de excepciones. La aplicación y la interpretación de dichas disposiciones de la Directiva 95/46/CE pueden diferir de un Estado miembro a otro.

53. A la luz de lo anterior, el SEPD puede aceptar las garantías incluidas en el Reglamento CPC, en concreto, que todas las transmisiones de terceros países estén sujetas tanto (i) al consentimiento de la autoridad competente que envió inicialmente la información como (ii) a la legislación comunitaria en materia de protección de datos aplicable.

54. Al SEPD le complace asimismo que las Directrices de protección de datos CPC recomienden que — a menos que el tercer país garantice un nivel adecuado de protección — los acuerdos bilaterales de asistencia deberán establecer garantías adecuadas de protección de los datos y, cuando así se requiera, el acuerdo deberá ser notificado a las autoridades de control de protección de datos pertinentes.

55. Dicho esto, las medidas establecidas en el Reglamento CPC no son ideales. Su aplicación es compleja ya que la autoridad competente que esté decidiendo si transmite información a un tercer país deberá tener en cuenta no solo su propio acuerdo bilateral con dicho tercer país, su legislación sobre protección de datos y su propia valoración de la adecuación de la transmisión de datos al tercer país en cuestión, sino también si las otras autoridades competentes implicadas que han contribuido al expediente (y pueden ser varias) han dado o no su consentimiento, sobre la base de su propia legislación sobre protección de datos.

56. Desde el punto de vista de la protección de datos, esta complejidad provoca incertidumbre en cuanto a los derechos de los interesados y, en particular, sobre si procede transmitir sus datos al extranjero y en qué condiciones. Los interesados tampoco se benefician, en la mayor medida posible, de una legislación comunitaria sobre protección de datos sólida y armonizada. Además, desde el punto de vista de las autoridades competentes, también es probable que esta complejidad dificulte la cooperación entre las autoridades competentes y suponga una carga administrativa.

57. A la luz de lo anterior, el SEPD anima a que se celebren acuerdos a escala comunitaria que proporcionen garantías de protección de datos adecuadas mientras que, al mismo tiempo, ayudan a que se evite la aplicación de criterios heterogéneos y el resultante aumento de la carga administrativa para las autoridades competentes.

5.2. Acuerdos a escala comunitaria

58. Además de la posibilidad prevista en el artículo 14 de una cooperación bilateral, el artículo 18 del Reglamento CPC sobre acuerdos internacionales establece también que «la Comunidad cooperará con terceros países y con las organizaciones internacionales competentes» y que «las disposiciones en materia de cooperación, incluida la adopción de medidas de asistencia mutua, podrán ser objeto de acuerdos entre la Comunidad y las terceras partes en cuestión».

([14]) La Comisión también debería considerar, en su caso, realizar al menos una evaluación de impacto parcial en materia de protección de datos e intimidad, sobre el fin, la duración y las modalidades del período de conservación, así como analizar otras cuestiones pendientes que no se han tratado todavía de manera global.

([15]) Véase el apartado 6.3 del Dictamen del SEPD de 14 de enero de 2011 mencionado anteriormente.

59. Por los motivos explicados en el apartado 5.1, el SEPD apoya a la Comisión en su iniciativa para negociar y celebrar acuerdos a escala comunitaria, con las garantías de protección adecuadas, armonizados a nivel de la Unión, que sustituyan los acuerdos bilaterales existentes.

60. Este apoyo se encuentra, no obstante, condicionado a que la Comisión y los legisladores europeos se comprometan a garantizar el máximo nivel de protección para los intercambios de datos personales con terceros países. Las implicaciones de los acuerdos de cooperación internacionales con terceros países deberán considerarse con atención desde el punto de vista de la protección de datos, debiéndose establecer normas claras que regulen estos intercambios así como garantías de protección de datos adecuadas, consultando con el SEPD y, en su caso, con las autoridades nacionales de protección de datos.

61. A pesar de que el artículo 18 del Reglamento CPC no trata específicamente la cuestión del acceso directo al CPCS por parte de las autoridades de los terceros países, esta situación es técnicamente posible. El SEPD no quiere desalentar la inclusión de nuevas funcionalidades en el CPCS que permitan a las autoridades competentes de los terceros países un acceso estrictamente limitado y selectivo a través de un mecanismo diseñado específicamente (canal de comunicación e interfaz), que podría, de hecho, aumentar la eficacia de la cooperación.

62. Dicho esto, tal acceso directo tiene sus propios riesgos y, por tanto, sus implicaciones en materia de protección de datos y deberían adoptarse las medidas técnicas y organizativas y las garantías necesarias. Todas las funcionalidades técnicas deben construirse aplicando los principios de «intimidad mediante el diseño». La seguridad también debería ser una prioridad clara. Por último, el SEPD debería ser consultado, en su caso, así como las autoridades nacionales de protección de datos.

VI. «DERECHOS DE PROTECCIÓN DE LOS DATOS DE LOS CONSUMIDORES» Y COOPERACIÓN REFORZADA, A TRAVÉS DEL CPCS, DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS

63. Siempre que se sigan sus recomendaciones (incluidas también las indicadas en el dictamen del control previo), el SEPD confía que el CPCS puede ser una herramienta eficaz y favorable para la protección de datos en una aplicación transfronteriza contra las violaciones de derechos de los consumidores en el mercado interior.

64. Con el desarrollo del comercio electrónico y el uso creciente de las redes de comunicaciones electrónicas por parte de los consumidores de diversos productos y servicios, cada vez se procesarán más datos de personas cuando actúan como consumidores. De este modo, los consumidores se enfrentan de manera creciente a las violaciones de sus derechos en materia de protección de datos. En consecuencia, existe la necesidad de que las autoridades de protección de datos cooperen de manera eficaz para detener dichas violaciones.

65. Entre las casos más comunes de violaciones de los «derechos de protección de los datos de los consumidores» están las comunicaciones comerciales no solicitadas (spam), el robo de identidad, la publicidad ilícita basada en el comportamiento y las violaciones de datos (violaciones de la seguridad).

66. Teniendo en cuenta que el número de casos de carácter transfronterizo es posible que crezca en la sociedad de la información, el SEPD anima a la Comisión a que considere las posibles medidas legislativas para proteger los «derechos de protección de los datos de los consumidores» y reforzar la cooperación transfronteriza entre las autoridades competentes, tanto de protección de datos como de protección de los consumidores.

67. En particular, y considerando también otras opciones posibles, debe considerarse atentamente si se permite a las autoridades de protección de datos un acceso personalizado al CPCS, para que cooperen entre ellas, así como con otras autoridades competentes que ya tienen acceso al CPCS.

68. El acceso por parte de las autoridades de protección de datos debe ser claramente limitado a lo que resulte necesario para realizar las tareas dentro de sus ámbitos de competencia y con arreglo a las sinergias que se identifiquen. Por supuesto también debería garantizarse que el marco de participación de las autoridades de protección de datos se diseñará teniendo en cuenta la independencia de las mismas.

VII. CONCLUSIONES

69. Al SEPD le complace que el CPCS tenga como base un fundamento jurídico que establece asimismo garantías de protección de datos específicas. Para tratar todas las cuestiones pendientes en materia de protección de datos, el SEPD destaca que en la próxima revisión del marco jurídico del CPCS deberán considerarse las recomendaciones que se resumen a continuación.

70. Mientras tanto, la adopción de medidas adicionales en el plano práctico, técnico y organizativo (tal como se ha recomendado en el dictamen de control previo) puede proporcionar una solución parcial provisional para abordar estas cuestiones. A la espera de cambios legislativos, también pueden introducirse algunos cambios a través de las Directrices operativas del CPCS.

71. En relación con el período de conservación, el SEPD recomienda que (i) las solicitudes de asistencia mutua deberían cerrarse dentro de los plazos específicamente designados (ii) salvo si está en curso una investigación o una aplicación, las alertas deberán retirarse y suprimirse en el plazo de seis meses desde su emisión (a menos que se justifique otro plazo de conservación más adecuado); y (iii) la Comisión deberá aclarar y reconsiderar el fin y la proporcionalidad de conservar todos los datos relativos a los casos cerrados durante otros cinco años.

72. Además, al SEPD le complace que la segunda modificación de la CPC aclare el acceso de la Comisión a los datos en el CPCS. En particular, al SEPD le complace que a la Comisión no tenga acceso a las comunicaciones confidenciales entre las autoridades competentes de los Estados miembros, como las solicitudes de asistencia mutua.

73. Asimismo, le complace que la segunda modificación CPC haya introducido una disposición que aborda el tratamiento de categorías de datos especiales en el CPCS.

74. Como puntos adicionales, el SEPD recomienda a la Comisión que vuelva a valorar las medidas técnicas y organizativas adicionales que debe adoptar para garantizar que la protección de datos y la intimidad están «diseñadas» en la arquitectura del sistema del CPCS («intimidad mediante el diseño») y que se adoptan los controles adecuados para garantizar el cumplimiento de la protección de datos y aportar pruebas de ello («rendición de cuentas»).

75. Asimismo, si debe celebrarse un acuerdo a escala comunitaria entre la Unión Europea y un tercer país para regular la cooperación en materia de protección de los consumidores, deberán considerarse con atención las implicaciones de dichas medidas y deberán establecerse normas claras que regulen estos intercambios y las garantías de protección de datos adecuadas.

76. Por último, el SEPD recomienda a la Comisión que estudie las posibles sinergias que pueden plantearse si se permite a las autoridades de protección de datos unirse a la comunidad de usuarios del CPCS en la cooperación para ayudar a reforzar los «derechos de protección de los datos de los consumidores».

Hecho en Bruselas, el 5 de mayo de 2011.

Giovanni BUTTARELLI

Asistente del Supervisor Europeo de Protección de Datos