GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

01910/2007/ES
WP 139

Dictamen 6/2007
sobre cuestiones de protección de datos relacionadas con el Sistema de Cooperación para la Protección de los Consumidores (SCPC)

Adoptado el 21 de septiembre de 2007

ÍNDICE

EL GRUPO DE TRABAJO SOBRE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

creado con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995,

Visto el artículo 29, el artículo 30, apartado 1, letra c), y el artículo 30, apartado 3, de la Directiva mencionada,

Visto su Reglamento interno y, en particular, sus artículos 12 y 14,

HA ADOPTADO EL PRESENTE DICTAMEN:

1. INTRODUCCIÓN

El presente dictamen del Grupo de Trabajo sobre protección de datos del artículo 29 (en lo sucesivo **"el Grupo de Trabajo"**) se refiere a las cuestiones de protección de datos relacionadas con el sistema de cooperación para la protección de los consumidores (en lo sucesivo **"el SCPC"**), que es la base de datos electrónica gestionada por la Comisión Europea para el intercambio de información entre las autoridades responsables de la protección de los consumidores en los Estados miembros y la Comisión, de acuerdo con las disposiciones del Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores (en lo sucesivo **"Reglamento CPC"**).

El presente dictamen responde a una carta de 30 de marzo de 2007 del Jefe de la Unidad B-5 "Aplicación de la legislación y recurso para los consumidores" de la Dirección General de Sanidad y Protección de los Consumidores de la Comisión Europea (en lo sucesivo **"DG SANCO"**), dirigida a la Secretaría del Grupo de Trabajo solicitando su dictamen.

El Grupo de Trabajo acoge con satisfacción la consulta, pero lamenta que la misma se le solicite después de la adopción del Reglamento CPC y de la Decisión 2007/76/CE de la Comisión de 22 de diciembre de 2006 (en lo sucesivo **"Decisión de aplicación del Reglamento CPC"**), y después de que el SCPC se haya creado, esté plenamente operativo y haya comenzado a funcionar. Si se le hubiera consultado antes, el Grupo de Trabajo habría podido proponer sus ideas en una fase en la que habría sido más fácil tener en cuenta sus recomendaciones.

Dicho esto, en general, el Grupo de Trabajo acoge con satisfacción el establecimiento de un sistema electrónico para el intercambio de información. En efecto, tal sistema modernizado puede no sólo aumentar la eficacia de la cooperación, sino que también, desde el punto de vista de la protección de datos, puede contribuir a garantizar la conformidad con las legislaciones vigentes en este ámbito, fijando un marco que defina claramente la información que puede intercambiarse, con quién y en qué condiciones.

Sin embargo, la creación de esta base de datos centralizada implica también algunos riesgos. El principal riesgo consiste en el hecho de que pueda intercambiarse aún más información y de forma más amplia de lo que es estrictamente necesario para una cooperación eficaz, y que los datos, algunos de los cuales pueden estar desfasados o ser inexactos, podrían permanecer en la base de datos más tiempo del necesario. La seguridad de una base de datos accesible a 27 Estados miembros representa también una cuestión delicada, puesto que la seguridad de todo el sistema depende del nivel de seguridad que pueda garantizar el eslabón más débil de la red.

El presente documento tiene por objeto identificar las principales preocupaciones en materia de protección de datos que podrían suscitar la creación y el funcionamiento del SCPC, y recomendar soluciones capaces de reducir estas preocupaciones.

El documento va dirigido tanto a la Comisión como a las autoridades competentes de los Estados miembros, en su calidad de responsables del tratamiento en el marco del SCPC, tal como se explicará más abajo. Además, las recomendaciones que se formulan en el documento deberían también servir de base para las futuras decisiones del "Comité regulador" compuesto por representantes de los Estados miembros, constituido de conformidad con lo dispuesto en el artículo 19 del Reglamento CPC, con la misión de asistir a la Comisión en la aplicación del Reglamento CPC. Por último, el presente documento va dirigido también a los legisladores de los Estados miembros, a los que el apartado 4 del artículo 13 del Reglamento CPC obliga a adoptar "las medidas legislativas necesarias para restringir los derechos y las obligaciones previstos en los artículos 10, 11 y 12 de la Directiva 95/46/CE en la medida que se requiera para salvaguardar los intereses contemplados en las letras d) y f) del apartado 1 del artículo 13 de dicha Directiva."

PARTE A: DESCRIPCIÓN DEL SISTEMA

2. OBLIGACIONES DE ASISTENCIA MUTUA PREVISTAS POR EL REGLAMENTO CPC

2.1. Objeto del Reglamento CPC: la cooperación entre las autoridades responsables de la protección de los consumidores. El Reglamento CPC se adoptó con el fin de mejorar la aplicación de la legislación que protege a los consumidores en el mercado interior. Este Reglamento crea, a escala de la Unión Europea, una red de autoridades nacionales encargadas de garantizar esta aplicación. Fija el marco y las condiciones generales de la cooperación entre los Estados miembros. En este nuevo sistema, cada autoridad podrá pedir la asistencia de las otras autoridades pertenecientes a la red para investigar posibles infracciones de la legislación de protección de los consumidores y para actuar con vistas a poner fin a prácticas comerciales engañosas destinadas a los consumidores que viven en otros países de la Unión Europea.

2.2. Ámbito de aplicación del Reglamento CPC: las infracciones intracomunitarias de directivas y reglamentos específicos. El ámbito de aplicación del Reglamento CPC se limita a las "infracciones intracomunitarias" de las directivas y reglamentos enumerados en el anexo del Reglamento CPC. Esta lista, que podrá actualizarse en caso necesario, contiene actualmente 15 directivas y reglamentos, incluidas las directivas relativas a la publicidad engañosa, la venta a distancia, el crédito al consumo, la radiodifusión televisiva, los viajes combinados, las cláusulas abusivas en los contratos, la multipropiedad, el comercio electrónico y otros ámbitos. Para estar reguladas por el Reglamento CPC, las "infracciones intracomunitarias" i) deben tener carácter "transfronterizo", y ii) deben perjudicar "los intereses colectivos de los consumidores".

2.3. Asistencia mutua en virtud del Reglamento CPC: investigación, ejecución y alertas. Los capítulos II y III del Reglamento CPC obligan a las autoridades competentes de los Estados miembros a prestarse mutuamente asistencia en materia de investigación y ejecución. Además, deben también informar a los otros Estados miembros y a la Comisión en caso de

sospecha o confirmación de una infracción intracomunitaria. Por último, tienen la obligación específica de coordinar sus actividades cuando los consumidores de más de dos Estados miembros se vean afectados por una infracción.

3. FINALIDAD, BASE JURÍDICA Y CREACIÓN DEL SCPC

3.1. Finalidad del SCPC: una base de datos para intercambiar información relacionada con la asistencia mutua. El SCPC es una base de datos electrónica gestionada por la Comisión Europea, concebida para ofrecer un sistema estructurado de intercambio de información entre las autoridades competentes de los Estados miembros, con el fin de cumplir su obligación de asistencia mutua prevista por el Reglamento CPC**.**

3.2. Esquema de las operaciones de tratamiento en el marco del SCPC. Los usuarios del sistema son la Comisión y las autoridades competentes de los Estados miembros. Además, se designa una "oficina de enlace única" en cada Estado miembro para garantizar la coordinación (véase el punto 5.3 *infra*).
Las autoridades competentes introducen los datos en el sistema. Por ejemplo, una autoridad competente puede enviar una solicitud de información o ejecución a otra autoridad competente. Puede también enviar una alerta a determinados Estados miembros y a la Comisión. Esta información se almacena en la base de datos y puede ser recuperada por otros usuarios destinatarios de la comunicación, por ejemplo la autoridad a la que se haya solicitado que lleve a cabo una medida de ejecución, o por la Comisión. Ésta realiza las supresiones de datos a petición de las autoridades de los Estados miembros, que deben informarla cuando los casos se cierran o cuando las alertas resultan infundadas. En caso de infracción confirmada que dé lugar a una medida de ejecución, los datos se conservan durante cinco años tras la notificación de la medida. Las normas sobre la conservación y la supresión de los datos se describen y examinan con más detalle en los puntos 6 y 11 *infra*.

3.3. Base jurídica del SCPC. La base jurídica del SCPC se encuentra en el artículo 10 del Reglamento CPC, que dispone que "la Comisión mantendrá actualizada una base de datos electrónica en la que registrará y tratará la información recibida con arreglo a los artículos 7, 8 y 9" de dicho Reglamento. Además, el apartado 3 del artículo 12 prevé que "las solicitudes de asistencia y toda comunicación de información se presentarán por escrito en un formulario tipo y se comunicarán por vía electrónica mediante la base de datos establecida en el artículo 10".

La lectura conjunta de estos artículos pone de manifiesto que las solicitudes de asistencia mutua, las alertas y las comunicaciones realizadas en virtud de los capítulos II y III del Reglamento CPC deben canalizarse a través del SCPC[1].

Además, la Decisión de aplicación del Reglamento CPC prevé que los Estados miembros informarán a la Comisión y a los demás Estados miembros, a través del foro de debate que se pondrá a su disposición en la base de datos, de todas las competencias adicionales en materia de investigación y aplicación que se atribuyan a las autoridades competentes y que no sean las establecidas en el artículo 4, apartado 6, del Reglamento CPC.

[1] No todas las actividades de cooperación e intercambios de información previstos por el Reglamento CPC deben pasar obligatoriamente por la base de datos del SCPC. Por ejemplo, el capítulo IV prevé una cooperación en materia de formación e intercambio de los responsables de la aplicación de la protección de los consumidores. Puesto que el intercambio de información vinculado a estas actividades no está incluido en el ámbito de aplicación del SCPC, no se aborda en el presente documento.

3.4. Decisión de aplicación del Reglamento CPC. Las disposiciones del Reglamento CPC aplicables al SCPC entraron en vigor el 29 de diciembre de 2006. Poco antes de esta fecha, la Comisión, asistida por un Comité regulador compuesto por representantes de los Estados miembros, adoptó una decisión de aplicación**.**

Esta Decisión determina los campos de datos que deben incluirse en la base de datos, así como el contenido mínimo de las solicitudes, de las respuestas y de las alertas. Prevé también los plazos de algunas etapas de los procedimientos de asistencia mutua y otras medidas de aplicación.

3.5. Creación del SCPC. La concepción del sistema sigue las disposiciones fijadas por el Reglamento CPC y por su Decisión de aplicación. Estas dos fuentes precisan las principales características y enumeran algunos aspectos de la base de datos. Sin embargo, no proporcionan un conjunto completo de directrices para su concepción, su gestión, su funcionamiento y su utilización. La Comisión concibió el SCPC tal como existe actualmente, en concertación con los Estados miembros y con un grupo de usuarios clave que representaban a las autoridades competentes en distintos Estados miembros.

Desde el punto de vista técnico, la Comisión construyó el sistema y es el operador. Los datos se albergan en servidores de la Comisión, y son sus técnicos quienes administran el sistema y garantizan su seguridad. Además, la Comisión también puede introducir modificaciones en el diseño del sistema, en caso necesario.

El SCPC ya está instalado y en funcionamiento, pero algunas características previstas por la Decisión de aplicación del Reglamento CPC están bloqueadas: en particular, los campos de datos que se refieren a los directores de empresa no se pueden utilizar actualmente, a la espera de que se clarifiquen los aspectos relacionados con el respeto de la protección de datos.

4. FLUJO DE DATOS EN EL MARCO DEL SCPC

El Reglamento CPC y la Decisión de aplicación, conjuntamente, establecen de forma detallada las categorías de información que pueden o deben intercambiarse a través del SCPC.

4.1. Disposiciones generales y confidencialidad. En general, la Decisión de aplicación del Reglamento CPC prevé que la autoridad competente que lanza una solicitud de asistencia mutua o una alerta debe proporcionar toda la información de que disponga y que pueda ser útil a otras autoridades competentes con el fin de responder a la solicitud de una manera eficaz o de garantizar un seguimiento adecuado de la alerta**.**

En el momento de responder a la solicitud de información, la autoridad requerida debe a su vez proporcionar toda la información mencionada por la autoridad requirente que sea necesaria para establecer si ha tenido lugar una infracción intracomunitaria o si existe una sospecha razonable de que pueda tener lugar. De la misma manera, en el momento de responder a una solicitud de ejecución, la autoridad requerida debe informar a la autoridad requirente de las acciones emprendidas o previstas y de los poderes ejercidos para responder a la solicitud. En los dos casos, si una autoridad competente se niega a responder a una solicitud, debe incluir en su respuesta una motivación de la denegación.

En cualquier caso, las autoridades requirentes y requeridas deben indicar si la información proporcionada debe recibir un tratamiento confidencial (véase también el punto 5.4 *infra*).

4.2. Alertas e información de retorno. El apartado 1 del artículo 7 del Reglamento CPC dispone que "cuando una autoridad competente tenga conocimiento de que se ha producido una infracción intracomunitaria, o tenga sospechas razonables de que tal infracción pueda producirse, lo notificará a las autoridades competentes de otros Estados miembros y a la Comisión y les enviará sin demora toda la información necesaria". Además, el apartado 2 del artículo 7 dispone que "cuando una autoridad competente adopte otras medidas de aplicación o reciba solicitudes de asistencia mutua con respecto a la infracción intracomunitaria, lo notificará a las autoridades competentes de otros Estados miembros y a la Comisión".

En la práctica, el artículo 7 implica el intercambio de dos tipos de información:

- **alertas:** un mensaje de alerta enviado por una autoridad a homólogos de la red en otros Estados miembros y a la Comisión para informarles de la existencia de una infracción de la legislación sobre protección de los consumidores o de una sospecha razonable de tal infracción;

- **información de retorno:** cuando las autoridades competentes adoptan otras medidas de ejecución o reciben solicitudes de asistencia mutua, informan a la Comisión y a otros homólogos de la red acerca de la solicitud recibida o de la acción de ejecución que se haya emprendido.

De acuerdo con la Decisión de aplicación del Reglamento CPC, el SCPC debería contener los campos de información siguientes para las alertas:

i) tipo de infracción intracomunitaria,
ii) estado de la infracción intracomunitaria (verificada, sospechas razonables),
iii) base jurídica,
iv) breve resumen,
v) cálculo del número de consumidores que pueden ser perjudicados y de los perjuicios económicos,
vi) requisitos, en su caso, de tratamiento confidencial,
vii) documentos adjuntos (en particular los relativos a declaraciones y otras pruebas).

Además, las alertas también deben contener los datos del vendedor o el proveedor responsable o sospechoso de ser responsable de una infracción intracomunitaria, tal como se describe en el punto 4.6 *infra*.

4.3. Cooperación en materia de ejecución. El apartado 1 del artículo 8 del Reglamento CPC dispone que, "a petición de la autoridad solicitante, la autoridad requerida adoptará todas las medidas de aplicación necesarias para poner término o prohibir inmediatamente la infracción intracomunitaria".

En la práctica, el intercambio de información con arreglo al artículo 8 incluye:

- **solicitudes de ejecución:** la solicitud de una autoridad a otra para que realice una acción destinada a hacer cesar una infracción confirmada.

Considerando las exigencias del apartado 3 del artículo 12 del Reglamento CPC, las respuestas se proporcionan también a través del SCPC, así como todas las comunicaciones a este respecto, mediante mensajes enviados a través del sistema.

La Decisión de aplicación del Reglamento CPC exige que la autoridad requirente proporcione a la autoridad requerida al menos: a) una identificación del comerciante o proveedor con respecto al cual se solicitan las medidas; b) datos relativos a la conducta o práctica en cuestión; c) la calificación jurídica de la infracción intracomunitaria con arreglo a la legislación aplicable, así como su base jurídica; y d) pruebas del perjuicio de los intereses colectivos de los consumidores, incluido, si es posible, el cálculo del número de consumidores que pueden ser perjudicados.

Esta Decisión de aplicación del Reglamento CPC prevé también que el SCPC deberá contener los siguientes campos de datos para las solicitudes de ejecución:

i) ubicación de los consumidores que puedan ser perjudicados,
ii) nombre del producto o servicio,
iii) código CCIF,
iv) base jurídica,
v) publicidad o soporte de venta utilizado,
vi) tipo de infracción intracomunitaria,
vii) estado de la infracción intracomunitaria (verificada, sospechas razonables),
viii) cálculo del número de consumidores que pueden ser perjudicados y de los perjuicios económicos,
ix) plazos de respuesta propuestos,
x) documentos adjuntos (en particular los relativos a declaraciones y otras pruebas) y requisitos, en su caso, de tratamiento confidencial,
xi) indicación de la asistencia solicitada,
xii) referencia a la alerta (si procede),
xiii) lista de las autoridades requeridas y Estados miembros afectados,
xiv) petición relativa a la participación de un funcionario competente en la investigación [artículo 6, apartado 3, del Reglamento (CE) no 2006/2004].

4.4. Coordinación de las actividades de vigilancia del mercado[2]. El apartado 1 del artículo 9 del Reglamento CPC, prevé que "las autoridades competentes coordinarán sus actividades de vigilancia del mercado y de aplicación de la legislación. Intercambiarán toda la información necesaria al efecto." El apartado 2 del artículo 9 añade lo siguiente: "cuando una autoridad competente tenga conocimiento de una infracción intracomunitaria que perjudique los intereses de los consumidores en más de dos Estados miembros, las autoridades competentes afectadas coordinarán sus acciones de aplicación de la legislación y sus solicitudes de asistencia mutua a través de la oficina de enlace única. En particular, intentarán coordinar temporalmente sus medidas de investigación y de aplicación." El apartado 3 del artículo 9 añade que "las autoridades competentes informarán a la Comisión por adelantado sobre las medidas de coordinación previstas en el párrafo anterior y podrán invitar a los funcionarios y otros acompañantes autorizados por la Comisión a participar en las reuniones de coordinación".

[2] El artículo 3, inciso i), del Reglamento CPC define las actividades de vigilancia del mercado como "las acciones de una autoridad competente encargada de detectar las infracciones intracomunitarias que se producen en su territorio".

En la práctica, el intercambio de información con arreglo el apartado 2 del artículo 9 incluye situaciones en las cuales están implicadas las autoridades competentes de al menos tres países. En este caso, puede intercambiarse información con el fin de detectar si ha tenido lugar una infracción. También se informa a la Comisión, que podrá, si las autoridades competentes se lo piden, participar en las investigaciones.

4.5. Intercambio de información previa solicitud. El apartado 1 del artículo 6 del Reglamento CPC dispone que, "a petición de la autoridad solicitante, la autoridad requerida […] facilitará sin demora toda la información pertinente solicitada para establecer si se ha producido una infracción intracomunitaria o para establecer si hay sospechas razonables de que pueda producirse". El apartado 2 del artículo 6, prevé por otro lado que "la autoridad requerida realizará, si fuera necesario con la asistencia de otras autoridades públicas, las investigaciones apropiadas o adoptará cualquier otra medida necesaria o apropiada […] para reunir la información solicitada".

El artículo 10 no hace expresamente referencia al artículo 6, sino que impone que determinados intercambios de información deberán realizarse exclusivamente a través del SCPC. No obstante, con arreglo al apartado 3 del artículo 12, que prevé que "las solicitudes de asistencia y toda comunicación de información se presentarán por escrito en un formulario tipo y se comunicarán por vía electrónica mediante la base de datos establecida en el artículo 10", todo intercambio de información con arreglo al artículo 6 deberá también efectuarse utilizando el SCPC.

En la práctica, el intercambio de información con arreglo al artículo 6 incluye:

- **solicitudes de información:** solicitud de una autoridad a otra para que le proporcione información útil que permita establecer si se ha producido una infracción de la legislación sobre protección de los consumidores o si hay sospechas razonables de que tal infracción pueda producirse.

Considerando las exigencias del apartado 3 del artículo 12 del Reglamento CPC, las respuestas se proporcionan también a través del SCPC, así como todas las comunicaciones a este respecto, mediante mensajes enviados a través del sistema.

La Decisión de aplicación del Reglamento CPC exige que la autoridad requirente deberá al menos: a) informar a la autoridad requerida de la naturaleza de la supuesta infracción comunitaria y de su base jurídica; b) aportar elementos suficientes para identificar la conducta o la práctica objeto de investigación; y c) especificar la información solicitada.

Esta Decisión prevé también los campos de datos que deberá contener el SCPC por lo que se refiere a las solicitudes de información. Son idénticos a los mencionados respecto de las solicitudes de ejecución en el punto 4.3 *supra*.

4.6. Datos del comerciante o proveedor responsable de una infracción intracomunitaria efectiva o supuesta. La Decisión de aplicación del Reglamento CPC dispone que el SCPC deberá incluir los campos de datos siguientes por lo que se refiere al vendedor o proveedor responsable o sospechoso de la infracción:

i) nombre,
ii) otros nombres comerciales,
iii) nombre de la sociedad matriz, en su caso,

iv) tipo de actividad empresarial,
v) domicilio(s) postal(es),
vi) dirección de correo electrónico,
vii) número de teléfono,
viii) número de fax,
ix) sitio web,
x) dirección IP,
xi) nombre o nombres del director o directores de la empresa, en su caso.

4.7. Foro de debate. Tal como se indica en el punto 3.3 *supra*, el SCPC incluye también un "foro de debate". Este foro se crea de conformidad con la Decisión de aplicación del Reglamento CPC con el único fin de intercambiar información relativa a los poderes de ejecución suplementarios que las autoridades competentes puedan haber recibido. El foro, como su nombre indica, es un foro de debate estructurado y la Decisión no impone ningún campo de datos obligatorio**.**

4.8. Tratamiento de datos relativos al personal. La Comisión trata también una cantidad limitada de datos personales (nombres, datos de contacto, lenguas habladas) relativos al personal que trabaja para las autoridades competentes y para las oficinas de enlace de los Estados miembros. Las operaciones de tratamiento de estos datos constituyen sin embargo un aspecto marginal del SCPC. Además, estas operaciones de tratamiento son inherentes a la gestión de todas las bases de datos con múltiples usuarios. Por esta razón no se profundizará en ellas en el presente documento.

5. ACCESO A LOS DATOS EN EL SCPC

5.1 Acceso de la Comisión a los datos

Acceso de la Comisión a los datos en virtud del Reglamento CPC. Tal como se ha descrito en el punto 4 *supra*, en virtud del Reglamento CPC, la Comisión debería tener acceso a lo siguiente:

- alertas (artículo 7, apartado 1),
- información de retorno (artículo 7, apartado 2; artículo 8, apartado 6; y artículo 10 apartado 2),
- en determinados casos, también a otra información vinculada al caso en cuestión (artículo 8, apartado 5; artículo 9, apartado 3; y artículo 15, apartado 5[3].

No obstante, según el Reglamento CPC, la Comisión no debe recibir:

- las solicitudes de información contempladas en el artículo 6,
- las solicitudes de ejecución contempladas en el artículo 8.

[3] Si la Comisión participa en investigaciones transfronterizas que implican a más de dos países, con arreglo al artículo 9, apartado 3, y previa invitación de las autoridades competentes, deberá recibir información sobre el caso en cuestión. Además, con arreglo al artículo 8, apartado 5 y al artículo 15, apartado 5, la Comisión deberá también tener acceso a determinada información relativa a las solicitudes de asistencia mutua siempre que deba contribuir a resolver conflictos entre autoridades requirentes y requeridas.

Estas solicitudes de asistencia mutua van dirigidas solamente a las autoridades competentes de los Estados miembros.

Acceso de la Comisión a los datos en virtud del documento de debate de la Comisión. De acuerdo con la descripción del documento de debate, los funcionarios de la Comisión responsables del seguimiento de la aplicación de uno o varios actos legislativos previstos por el Reglamento CPC, y solamente para los asuntos correspondientes al ámbito de esos actos, recibirán acceso únicamente de lectura para consultar la información relativa a la ejecución de las acciones con arreglo al artículo 8, apartado 6, del Reglamento CPC. El documento de debate de la Comisión no menciona la información de retorno por lo que se refiere a las solicitudes de información o a las alertas (artículo 7, apartado 2, y artículo 10, apartado 2), aunque probablemente estos flujos de información también figuran en la base de datos.

El documento de debate de la Comisión menciona también que los funcionarios de la Comisión que trabajan en la unidad responsable de la aplicación del Reglamento CPC tendrán acceso a toda la demás información contenida en la base de datos. Actualmente sólo utilizan estos datos para realizar el seguimiento de la aplicación del Reglamento CPC, en particular para extraer datos con fines estadísticos. A primera vista, eso deja suponer que, contrariamente a las disposiciones del Reglamento CPC, estos funcionarios de la Comisión disponen de un acceso ilimitado al SCPC, incluso a las solicitudes de información y a las solicitudes de ejecución intercambiadas entre las autoridades competentes de los Estados miembros y a todos los datos registrados como confidenciales (véase el punto 5.4 *infra*). La información suplementaria proporcionada por la DG SANCO durante la preparación del presente dictamen confirmó sin embargo que no es el caso. La DG SANCO confirmó expresamente que ningún funcionario de la Comisión tiene acceso a las solicitudes de información o a las solicitudes de ejecución intercambiadas entre las autoridades competentes de los Estados miembros, y que el acceso de la Comisión a los datos registrados como confidenciales está limitado, tal como se indica en el punto 5.4 *infra*.

Por último, según el documento de debate, los funcionarios de la Comisión pueden también participar en investigaciones coordinadas o en acciones de ejecución con arreglo al artículo 9, apartado 3 del Reglamento CPC. Estos funcionarios gozan de un acceso total a la información relacionada con los casos en cuestión.

5.2. Acceso de las autoridades competentes a los datos. Cuando las autoridades competentes introducen información en el sistema en forma de alertas, solicitudes de información o solicitudes de ejecución, les corresponde a ellas decidir a qué otras autoridades competentes conceden acceso a esta información. Por ejemplo, las autoridades competentes belgas pueden enviar únicamente a Francia y Luxemburgo una alerta pertinente para estos tres países, pero no para los otros Estados miembros. Lo mismo sucede con la información de retorno y las otras comunicaciones efectuadas a través de la base de datos.

5.3. Acceso a los datos por parte de las oficinas de enlace únicas. De acuerdo con el Reglamento CPC, las solicitudes de asistencia mutua (tanto las solicitudes de información como las solicitudes de ejecución) se envían a través de las oficinas de enlace únicas de las autoridades solicitante y requerida de los Estados miembros. La información transmitida a raíz de la solicitud se comunicará directamente a la autoridad solicitante y simultáneamente a las oficinas de enlace únicas pertinentes de las autoridades solicitante y requerida. Si la cooperación implica a más de dos Estados miembros, estas oficinas desempeñarán un papel

suplementario de coordinación. En todos estos casos, las oficinas de enlace únicas pueden tener acceso a datos personales, siempre que estén incluidos en las solicitudes de asistencia mutua y en las correspondientes respuestas. Sin embargo, estas oficinas no tienen acceso a la información registrada como confidencial (véase el punto 5.4).
Además, hay que tener en cuenta que numerosas oficinas de enlace únicas pueden ejercer dos funciones: por una parte, ejercen sus funciones de coordinación como oficinas de enlace únicas y, por otra parte, actúan también como autoridades competentes por lo que se refiere a determinadas infracciones de la protección de los consumidores. En esta última calidad, tienen acceso a los datos de la misma manera que cualquier otra autoridad competente.

5.4. Información registrada como confidencial. El apartado 3 del artículo 13 del Reglamento CPC dispone que la información almacenada en el SCPC y cuya difusión pudiera poner en peligro: i) la protección de la intimidad e integridad de la persona, ii) los intereses comerciales de una persona física o jurídica, iii) procedimientos judiciales y asesoría jurídica, o iv) la finalidad de inspecciones o investigaciones, será confidencial, a no ser que su difusión resulte necesaria para que se lleve a cabo la cesación o la prohibición de una infracción intracomunitaria y la autoridad que comunica la información esté de acuerdo con que se difunda.

La Decisión de aplicación del Reglamento CPC, según lo descrito en el punto 4, exige que las autoridades que introducen información o solicitudes de ejecución o alertas indiquen si la información debe tratarse de forma confidencial. Del mismo modo, al proporcionar información, la autoridad requerida también debe indicar si esta información debe tratarse confidencialmente. La Decisión de aplicación del Reglamento CPC exige también que el SCPC incluya campos de datos específicos para indicar que los datos intercambiados deben recibir un tratamiento confidencial. Según el documento de debate de la Comisión, una autoridad competente puede desear registrar una información como confidencial, por ejemplo cuando adjunta un documento a su mensaje y este documento adjunto contiene información confidencial.

Al igual que entre la Comisión, las autoridades competentes y las oficinas de enlace únicas, la Decisión de aplicación del Reglamento CPC dispone que el hecho de registrar datos como "confidenciales" implica también que las oficinas de enlace únicas no tendrán acceso a estos datos. Durante la preparación del presente dictamen, la DG SANCO precisó claramente que su intención es limitar de igual modo el acceso de la Comisión a la información registrada como confidencial[4].

Además, según el documento de debate de la Comisión, en algunos casos algunos documentos tampoco pueden revelarse a "organismos con intereses legítimos en la cesación o la prohibición de infracciones intracomunitarias", designados sobre la base de las disposiciones del Reglamento CPC con el fin de asistir a las autoridades competentes en las cuestiones de ejecución. De acuerdo con la Decisión de aplicación del Reglamento CPC, la revelación de información a estos organismos debería someterse a la aprobación previa de la autoridad solicitante, precisando la naturaleza y los detalles de la información que puede revelarse a este organismo.

[4] Este principio admite algunas excepciones. La información confidencial, si fuere necesario, puede utilizarse siempre que la Comisión deba resolver conflictos y siempre que participe en una investigación (véase el artículo 8, apartado 5; el artículo 9, apartado 3; y el artículo 15, apartado 5, del Reglamento CPC).

El tratamiento confidencial no impide sin embargo que las autoridades competentes puedan compartir datos confidenciales o que estos datos puedan transferirse a tribunales o a otras autoridades públicas. De momento, el texto del Reglamento CPC y la Decisión de aplicación tampoco limitan el acceso de la Comisión a estos datos.

6. PERIODOS DE CONSERVACIÓN EN VIRTUD DEL REGLAMENTO CPC Y DE LA DECISIÓN DE APLICACIÓN DEL REGLAMENTO CPC

6.1. Retirada de las alertas. El apartado 2 del artículo 10 del Reglamento CPC dispone que "cuando una autoridad competente establezca que una notificación de una infracción intracomunitaria comunicada conforme al artículo 7 se ha revelado ulteriormente infundada, retirará la notificación y la Comisión sin demora suprimirá la información correspondiente de la base de datos."

En la práctica, esto significa que la autoridad competente que haya introducido una alerta con arreglo al artículo 7 deberá retirarla, y que la información debe suprimirse de la base de datos en cuanto la autoridad competente establezca que la alerta era infundada.

6.2. Casos cerrados después de su ejecución. Con arreglo al apartado 6 del artículo 8, "la autoridad requerida informará sin demora a la autoridad solicitante, a las autoridades competentes de los demás Estados miembros y a la Comisión las medidas adoptadas y el efecto de éstas en la infracción intracomunitaria y también si dicha infracción ha cesado." El apartado 2 del artículo 10, dispone a continuación que "los datos almacenados en relación con la infracción intracomunitaria se borrarán a los cinco años de la notificación".

En la práctica, eso significa que la autoridad requerida debe notificar a la Comisión las medidas de ejecución adoptadas y que la información debe suprimirse de la base de datos cinco años después de esta notificación.

6.3. Casos cerrados después de las solicitudes de información. La Decisión de aplicación del Reglamento CPC dispone que la autoridad solicitante debe informar a la Comisión y suprimir la información de la base de datos a raíz de una solicitud con arreglo al artículo 6, si: a) la información intercambiada no genera una alerta o una solicitud en virtud del artículo 8; o b) se establece que no se ha producido ninguna infracción intracomunitaria.

En la práctica, esto significa que la autoridad solicitante debe informar a la Comisión si la solicitud de información no desemboca en una acción posterior de cooperación, como el envío de una solicitud de ejecución o de una alerta, o si se establece que no ha tenido lugar ninguna infracción del Reglamento CPC. La información debe entonces suprimirse de la base de datos.

7. LA ARQUITECTURA DE SEGURIDAD DEL SCPC

7.1. El centro de datos de la Comisión. La Comisión proporciona la infraestructura técnica del SCPC, incluidos el apoyo técnico y el servicio de ayuda al usuario. Los datos recogidos se almacenan en servidores del centro de datos de la Dirección General de Informática, en Luxemburgo. Este servidor funciona con arreglo a las decisiones y las disposiciones de la Comisión en materia de seguridad adoptadas por la Dirección de Seguridad. Se aplica el

sistema general de protección de las telecomunicaciones y de la informática de la Comisión Europea.

El SCPC está protegido por sistemas de detección de intrusiones y contra los virus, correo electrónico no deseado y otros tipos de amenazas. Está asegurado por un cortafuegos y por un servidor proxy situados y gestionados por el centro de telecomunicaciones DIGIT de la Comisión. Todas las transacciones se codifican a través del canal https. El sistema sigue las normas de protección y recuperación del centro de datos de la Comisión Europea.

7.2. La red TESTA II. La información no se intercambia por Internet, sino a través de la red de telecomunicaciones seguras TESTA II, que conecta los organismos e instituciones comunitarias con las autoridades nacionales. TESTA II es una red privada y cerrada. La Comisión garantiza la seguridad hasta los puntos de contacto nacionales. El acceso a esta columna vertebral de la red se efectúa a través de puntos de conexión identificados. Todo el tráfico de esta red está codificado. La migración hacia s-TESTA, actualmente en curso, aportará una mayor seguridad**.**

Desde los puntos de contacto nacionales hasta los usuarios, los Estados miembros respectivos son responsables de la construcción física de la conexión y de la vigilancia de su seguridad. Cada país debe garantizar que solamente el personal autorizado pueda acceder a TESTA. La red no posee ninguna "ventana" a Internet. Sólo es accesible por los usuarios predefinidos y solamente a través de aquellos ordenadores que estén conectados físicamente a la red y estén instalados en las oficinas de las autoridades nacionales y de la Comisión.

7.3. Acceso a los datos. Existen diferentes perfiles de acceso al SCPC. Estos perfiles vienen determinados por los derechos de acceso a los datos almacenados en la base de datos. Las autoridades competentes comunican el nombre de sus usuarios a la Comisión. Cada autoridad competente cuenta con al menos un usuario. El acceso al SCPC sólo se concede a un grupo de usuarios bien definidos e identificables. Cada acceso es nominativo y está vinculado a una única persona. No se autorizan usuarios funcionales**.**

Para acceder a la aplicación, es necesario disponer de un nombre de usuario y de una contraseña. La oficina de enlace única de cada país solicita los nombres de usuario a la Comisión. Ésta crea la clave de acceso y la contraseña inicial que se transmite al usuario a través de la oficina de enlace única. El usuario debe modificar esta contraseña en su primera conexión. La nueva contraseña debe ser una contraseña segura, es decir, debe constar de al menos 8 caracteres y ser alfanumérica. Se ha previsto mejorar este sistema: a partir de finales de año, la cadena de caracteres deberá contener al menos tres tipos de caracteres de entre cuatro familias de caracteres (letras minúsculas, letras mayúsculas, cifras y caracteres especiales).

El documento de debate de la Comisión insiste en que la combinación de las medidas anteriormente mencionadas con una red privada sitúa el acceso al SCPC en un nivel de seguridad adecuado en relación a la naturaleza de los datos almacenados y transferidos a través del SCPC.

Ya es posible una mayor extensión de la seguridad a nivel nacional. Si un país decide utilizar, por ejemplo, un equipo de autenticación codificada con chip, éste puede integrarse fácilmente a nivel nacional porque los procedimientos de acceso al sistema se deciden en los Estados miembro y ellos son responsables del funcionamiento y la seguridad del sistema a partir de los puntos de contacto nacionales TESTA II.

PARTE B: ANÁLISIS

8. RESPONSABLES DEL TRATAMIENTO DE LOS DATOS, LEGISLACIÓN APLICABLE Y AUTORIDADES DE CONTROL

8.1. El Reglamento CPC designa responsables del tratamiento de los datos a las autoridades competentes y a la Comisión. El artículo 2, letra d) de 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 (en lo sucesivo "Directiva 95/46/CE") y el artículo 2, letra d), del Reglamento (CE) n° 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 (en lo sucesivo " Reglamento (CE) n° 45/2001") disponen ambos que, cuando los fines y los medios del tratamiento estén determinados por un acto comunitario concreto, el responsable del tratamiento o los criterios específicos aplicables a su nombramiento podrán determinarse en tal acto comunitario.

Este es el caso del SCPC, cuyos fines y medios de tratamiento están definidos por el Reglamento CPC, cuyo artículo 10 dispone expresamente que la Comisión y las autoridades competentes actuarán como responsables del tratamiento en relación con sus responsabilidades conforme al Reglamento CPC.

En particular, el artículo 10 dispone lo siguiente: "En relación con su responsabilidad de notificar la información que se vaya a almacenar en la base de datos y el tratamiento de datos personales que ello conlleve, las autoridades competentes serán consideradas responsables del tratamiento de acuerdo con la letra d) del artículo 2 de la Directiva 95/46/CE. En relación con sus responsabilidades conforme al presente artículo, y al tratamiento de datos personales que conlleven, la Comisión será considerada responsable del tratamiento de conformidad con la letra d) del artículo 2 del Reglamento (CE) no 45/2001."

8.2. Las autoridades competentes como responsables del tratamiento. Cada autoridad competente es responsable del tratamiento con respecto a sus propias actividades de tratamiento de los datos como usuario del sistema para sus propias finalidades, tal como prevé el Reglamento CPC. Deberá cumplir su propia legislación nacional en materia de protección de datos y estará sometida a la supervisión de sus propias autoridades nacionales encargadas de esta protección.

8.3. Las oficinas de enlace únicas como responsables del tratamiento. Como se ha visto en los puntos 5.3 y 5.4, las oficinas de enlace únicas también reciben información, excepto la información registrada como confidencial, con el fin de cumplir su función de coordinación por lo que respecta a la transmisión de la información y las solicitudes de ejecución. En este marco, deben ajustarse a su propia legislación nacional en materia de protección de datos y están sometidas a la supervisión de sus propias autoridades nacionales encargadas de esta protección.

8.4. El papel sui generis de la Comisión. El Reglamento CPC designa a la Comisión como responsable del tratamiento de los datos por lo que se refiere a sus propias tareas y responsabilidades. Habida cuenta de estas misiones y responsabilidades, que incluyen a la vez i) el funcionamiento del SCPC en beneficio de las autoridades competentes de los Estados miembros, y ii) su propia utilización del SCPC, la Comisión posee un papel sui generis, que no puede definirse fácilmente. Es importante que se reconozca la naturaleza sui generis de este papel, y que las tareas y las responsabilidades en materia de respeto de la protección de datos estén claramente distribuidas entre la Comisión y las autoridades competentes.

Las actividades de la Comisión están reguladas por el Reglamento (CE) n° 45/2001 y están sometidas al control del Supervisor Europeo de Protección de Datos (en lo sucesivo **"SEPD"**).

9. BASE JURÍDICA

9.1. Aplicabilidad de la Directiva 95/46/CE y del Reglamento (CE) n° 45/2001. El SCPC se utiliza para el tratamiento de los datos de los vendedores y proveedores sospechosos de cometer infracciones a la legislación relativa a la protección de los consumidores. Estos vendedores y proveedores pueden ser sociedades, pero, más importante desde el punto de vista de la protección de datos, puede también tratarse de personas físicas. Además, la Decisión de aplicación del Reglamento CPC establece campos de datos específicos para el intercambio de información acerca de los directores de los vendedores o proveedores sospechosos. Por último, los datos personales relativos a otros individuos, por ejemplo propietarios o empleados de los vendedores o proveedores, denunciantes, agentes o testigos pueden aparecer también en los documentos adjuntos y breves resúmenes, que también se prevén específicamente en la Decisión de aplicación del Reglamento CPC. Por tanto, no cabe duda de que la utilización del SCPC implica un tratamiento de los datos personales en el sentido de lo dispuesto en el artículo 2, letra a), de la Directiva 95/46/CE y en la disposición correspondiente del Reglamento (CE) n° 45/2001.

9.2. Base jurídica y legalidad del tratamiento. El artículo 7, letra c) de la Directiva 95/46/CE prevé que el tratamiento de datos personales sólo podrá efectuarse si "es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento". El artículo 7, letra e), autoriza también el tratamiento si "es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos". El artículo 5, letras a) y b), del Reglamento (CE) n° 45/2001 contiene disposiciones similares.

Artículo 7, letra c): obligación legal de los responsables del tratamiento. Como se ha visto en el punto 3.3, el Reglamento CPC es la base jurídica del SCPC. Impone también la obligación a todas las autoridades competentes de intercambiar los datos relativos a la asistencia mutua exclusivamente a través de la base de datos. El Reglamento CPC es directamente aplicable a las autoridades competentes de todos los Estados miembros.

Artículo 7, letra e): realización de una tarea de interés público. El SCPC participa en la lucha contra las infracciones transfronterizas de la legislación europea sobre protección de los consumidores, en particular facilitando la coordinación de las actividades de las distintas autoridades competentes en distintos Estados miembros. Se trata de una misión de interés público. La cuestión de la "necesidad" se aborda en el punto 10.1 *infra*.

Por tanto, el Grupo de Trabajo considera que el artículo 7, letras c) y e), de la Directiva 95/46/CE puede considerarse una base jurídica adecuada para el tratamiento de los datos.

10. CALIDAD DE LOS DATOS

10.1. Limitación de la finalidad, imposibilidad de utilización posterior para una finalidad incompatible. De conformidad con lo dispuesto en el artículo 6, apartado 1, letra b), de la Directiva 95/46/CE, se dispondrá que los datos personales sean "recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines". El Reglamento (CE) n° 45/2001 contiene una disposición similar**.**

Limitación de la finalidad fijada por el Reglamento CPC. El apartado 1 del artículo 13 del Reglamento CPC prevé que "la información comunicada sólo podrá utilizarse para asegurar el respeto de la legislación protectora de los intereses los consumidores". El apartado 2 del artículo 13, añade que "las autoridades competentes podrán utilizar como prueba cualquier información, documento, constatación, declaración, copia certificada conforme o información comunicada sobre la misma base que los documentos análogos obtenidos en su propio país".

El Grupo de Trabajo acoge con satisfacción la limitación de la finalidad fijada para la utilización de los datos. No obstante, destaca que las finalidades permitidas y cualquier limitación de uso deben definirse de una manera más precisa a nivel operativo. Por esta razón, el Grupo de Trabajo hace las siguientes recomendaciones:

La utilización por las autoridades competentes debería limitarse a una cooperación específica caso por caso. Un riesgo inherente a las grandes bases de datos electrónicas de este tipo es que se utilicen para buscar sistemáticamente a individuos y "clasificarlos" en función de los resultados de la investigación. Habida cuenta de que tal uso no está previsto en el Reglamento CPC y que no existe ninguna protección a este respecto, el Grupo de Trabajo recomienda que la información contenida en la base de datos sólo se utilice en relación con cada investigación o ejecución del caso específico para el que se haya emitido una solicitud de asistencia mutua o una alerta en primer lugar, a menos que en una nueva Decisión de aplicación del Reglamento CPC se prevean específicamente usos suplementarios y se establezcan garantías adecuadas para la protección de datos.

Las finalidades para las cuales la Comisión puede utilizar los datos deberían precisarse claramente. En algunos casos, la propia Comisión utiliza los datos para los fines precisados en el Reglamento CPC, en particular para asistir a las autoridades competentes en determinados conflictos o para participar en investigaciones coordinadas que implican a más de dos países (véase el punto 10.2). Se trata de usos permitidos, definidos en el Reglamento CPC.

Sin embargo, en general, el Reglamento CPC no precisa cuál debería ser la finalidad del uso y el acceso de la Comisión a los datos. Este el caso tanto por lo que se refiere a la alerta y a la información de retorno. Se supone que la Comisión tendrá acceso a estos datos para que pueda: i) supervisar la aplicación del Reglamento CPC; ii) supervisar la aplicación de la legislación específica relativa a la protección de los consumidores cubierta por el Reglamento CPC (las directivas y reglamentos enumerados en su anexo); y iii) reunir información estadística relacionada con la realización de estas tareas. Estos usos están permitidos. Sin embargo, la Comisión debería garantizar que los datos personales que figuran en la alerta y en

la información de retorno que recibe no se utilicen para fines suplementarios no especificados. Éstos deberían especificarse claramente en una nueva Decisión de aplicación del Reglamento CPC, y la arquitectura del SCPC debería también configurarse de nuevo en consecuencia.

10.2. Necesidad y proporcionalidad

De conformidad con lo dispuesto en el artículo 6, apartado 1, letra c), de la Directiva 95/46/CE, los datos personales deben ser "adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente".

Introducciones de datos facultativas y predefinidas; acceso limitado a la base de datos. En primer lugar, el Grupo de Trabajo acoge con satisfacción el hecho de que la Decisión de aplicación del Reglamento CPC elabore una lista definida de los campos de datos que pueden incluirse en la base de datos. En segundo lugar, también acoge con satisfacción que la Decisión no exija que todos los campos de datos se rellenen cada vez, sino que más allá de unos requisitos mínimos esenciales, deja a la autoridad competente que introduce los datos la decisión de qué campos de datos rellenará y con qué nivel de detalle. En tercer lugar, el Grupo de Trabajo acoge con satisfacción el hecho de que solamente las autoridades competentes designadas por cada Estado miembro tienen acceso al SCPC y, de estas autoridades, solamente los agentes especialmente designados.

Análisis de la proporcionalidad caso por caso. El Grupo de Trabajo también acoge con satisfacción el hecho de que la lista de campos de datos parece en conjunto razonable y no excesiva para los fines perseguidos por el SCPC (las excepciones y motivos de preocupación se mencionarán más abajo).

Dicho esto, el Grupo de Trabajo no puede determinar de antemano si la utilización de todos los campos de datos es adecuada en todos los casos particulares. Además, algunos campos de datos están definidos tan ampliamente que depende casi totalmente del agente encargado de la ejecución que introduce los datos determinar en un caso concreto qué volumen de datos personales introducirá en la base de datos. Por ejemplo, un documento adjunto podrá contener copias de facturas que incluyan nombres de clientes y números de cuentas bancarias, o una lista de direcciones electrónicas de clientes a los que se hayan enviado mensajes de correo electrónico no deseado (*spam*). La conveniencia de incluir estos datos en la base dependerá del caso concreto.

Por esta razón, el Grupo de Trabajo señala que la "necesidad" y la "proporcionalidad" del tratamiento de los datos deben analizarse *in concreto*, para cada caso particular, cuando la información se introduzca o se recupere y se utilice.

En particular, las autoridades competentes deben garantizar, para cada información que se introduzca, que i) sólo se introduce la información personal que sea estrictamente necesaria en aras de una cooperación eficaz, y que ii) comparten la información solamente con las autoridades competentes de otros Estados miembros que necesiten tener acceso a la misma. Además, deben también garantizar que sólo conservarán los datos personales en la base de datos el tiempo necesario para la cooperación.

Formación de los agentes responsables de la ejecución, directrices para la utilización de la base de datos y medios técnicos para recordar la conformidad. Se trata de una evaluación que los agentes responsables de la ejecución deben realizar cada vez que

transfieran o traten la información. Estos agentes deberían tener conciencia de la importancia de realizar un análisis serio de la proporcionalidad caso por caso. Con el fin de garantizar que la Comisión y las autoridades competentes tratan los datos de acuerdo con el principio de calidad de los datos, el Grupo de Trabajo recomienda que la Comisión, como administradora del sistema, elabore una serie de directrices ("**directrices SCPC**") destinadas a los agentes responsables de la ejecución que tienen acceso al SCPC, describiendo las normas que deben seguirse con el fin de garantizar la conformidad con las normas de protección de datos. Estas directrices deben redactarse de tal modo que sean fácilmente comprendidas por personas que no tengan ningún conocimiento particular en el ámbito de la protección de datos. Pueden por ejemplo adoptar la forma de preguntas frecuentes en el SCPC y estar disponibles para todos los usuarios. Las directrices deberán cubrir todos los aspectos de la protección de datos del SCPC, pero haciendo especial hincapié en la cuestión del análisis de la proporcionalidad caso por caso.

Aunque corresponda a la Comisión elaborar las directrices del SCPC, son las autoridades competentes quienes, en definitiva, por lo que se refiere a la mayoría de las operaciones de tratamiento (por ejemplo, la introducción de información en el SCPC o la designación de los destinatarios de las alertas) y en virtud de su legislación nacional, siguen siendo responsables del cumplimiento de las obligaciones relativas a la protección de datos, incluida la realización de un análisis de proporcionalidad caso por caso. Por esta razón, con el fin de obtener un elevado nivel de conformidad, el contenido de las directrices y los elementos de protección de datos deberían también integrarse en la formación impartida a los agentes responsables de la ejecución por lo que se refiere a la utilización del SCPC.

Por último, en la medida en que resulte posible desde el punto de vista técnico y operativo, las características técnicas del SCPC deberán modificarse para incitar a los agentes responsables de la ejecución a evaluar los aspectos de la protección de datos cada vez que accedan a la base de datos. Una vez más, estas características deberán limitarse al aspecto de la proporcionalidad.

Información acerca de los directores. El Reglamento CPC no sugiere ni exige específicamente que la información relativa a los directores de los comerciantes o proveedores responsables de una infracción intracomunitaria efectiva o supuesta figuren en la base de datos. La Decisión de aplicación del Reglamento CPC exige sin embargo la creación de campos de datos para los nombres de los directores respecto de los intercambios de información, al igual que exige una entrada para la dirección y el número de teléfono del vendedor o el proveedor.

El Grupo de Trabajo reconoce que el intercambio de información relativa a los directores de los comerciantes o proveedores puede ser necesario en algunos casos. Por ejemplo, las mismas personas pueden utilizar una serie de sociedades como medio para realizar actividades fraudulentas. Por esta razón, los agentes responsables de la ejecución pueden tener necesidad legítima de intercambiar información sobre estas personas.

No obstante, el Grupo de Trabajo destaca que este intercambio de información plantea al mismo tiempo graves preocupaciones en materia de derecho a la intimidad.

En efecto, el hecho de incluir información acerca de los directores en el SCPC puede constituir graves violaciones del derecho a la intimidad y puede, en algunas situaciones, equivaler a acusarlos de ser "culpables por asociación", lo que podría tener un efecto

perjudicial sobre su reputación y sobre sus perspectivas profesionales. La Comisión es consciente de este problema y, hasta ahora, ha decidido bloquear esta función de la base de datos. Por esta razón, el Grupo de Trabajo recomienda que las directrices del SCPC prevean específicamente que los agentes responsables de la ejecución deberán evaluar en cada caso si la inclusión del nombre del director es adecuada o no.

Información acerca de los consumidores, demandantes y otros terceros en los "breves resúmenes" y los "anexos". Entre los campos de datos que pueden utilizarse en caso de alertas, solicitudes de información y solicitudes de ejecución, la Decisión de aplicación del Reglamento CPC incluye un campo para los "documentos adjuntos". Prevé también "breves resúmenes" en caso de alertas.

Es posible que los documentos adjuntos o los breves resúmenes contengan datos personales sobre los demandantes, clientes, testigos, empleados, propietarios, agentes u otros terceros. Por ejemplo, un anexo puede contener copias de facturas donde figuren nombres de clientes y números de cuentas bancarias, o una lista de direcciones electrónicas resultante del envío de mensajes de correo electrónico no deseado (*spam*).

La comunicación de algunos de estos documentos que incluyan datos personales puede justificarse en determinadas circunstancias. No obstante, el Grupo de Trabajo recomienda que, siempre que sea posible, los datos personales se retiren de los breves resúmenes y se borren o supriman de los documentos adjuntos (por ejemplo, tachando los nombres, direcciones o números de tarjetas de crédito). En caso de duda por lo que respecta a la necesidad de transferir información o documentos que contengan datos personales, el Grupo de Trabajo recomienda que se supriman los datos personales. En caso de que posteriormente resulte que el destinatario necesita una copia íntegra de un documento, por ejemplo con fines probatorios, siempre tendrá la posibilidad de pedir la información que falte a la parte que haya proporcionado inicialmente el documento. Estas recomendaciones deberían especificarse claramente en las directrices del SCPC.

Datos personales en el "foro de debate". Tal como se ha indicado en el punto 3.3 *supra*, la Decisión de aplicación del Reglamento CPC prevé que los Estados miembros deberán informar a la Comisión y a los otros Estados miembros a través de un "foro de debate" establecido en la infraestructura del SCPC, acerca de todas las competencias adicionales en materia de investigación y aplicación que se atribuyan a las autoridades competentes además de las requeridas específicamente en virtud del Reglamento CPC. Durante la elaboración del presente dictamen, la DG SANCO explicó que está previsto que el foro de debate se utilice sólo para el intercambio de información relativa a cuestiones tales como nuevos poderes de ejecución o mejores prácticas. Es pues improbable que estos intercambios de información incluyan datos personales. Es importante en cualquier caso destacar que este foro no debe servir para intercambiar datos vinculados a los casos analizados, y que no debería, por regla general, contener datos personales. Esto también deberá precisarse en las directrices del SCPC.

Sospechas "razonables". El Grupo de Trabajo destaca también que los datos relativos a las presuntas infracciones sólo deberían incluirse si estas "sospechas" son "razonables". La interpretación de la expresión "sospechas razonables" se deja a los Estados miembros, pero el Grupo de Trabajo destaca que no puede incluirse ningún dato en el SCPC si no existe al menos información significativa o alguna prueba de que ha tenido lugar una infracción. Se trata de otro aspecto que debe discutirse en las directrices del SCPC.

Los derechos de acceso de la Comisión deberían estar más limitados. Si bien la redacción del documento de debate de la Comisión suscitó inicialmente dudas a este respecto, parece que el acceso de la Comisión a los datos no va más allá de lo que requiere el Reglamento CPC.

El Grupo de Trabajo se acoge con satisfacción este aspecto y destaca la importancia de que el acceso de la Comisión esté limitado estrictamente a lo que prevé el Reglamento CPC. En particular, la Comisión no debería tener ningún acceso a las comunicaciones entre los Estados miembros acerca de las solicitudes de información con arreglo al artículo 6 o las solicitudes de ejecución con arreglo al artículo 8. Los planes de la DG SANCO de limitar (con algunas excepciones) el acceso de la Comisión a la información calificada como confidencial también son bienvenidos.

Tal como se ha visto en el punto 5.1, la información de retorno por lo que se refiere tanto a las solicitudes de información como de ejecución debe enviarse a la Comisión con arreglo al artículo 7, apartado 2, y al artículo 8, apartado 6, del Reglamento CPC. Esta información de retorno contiene probablemente suficientemente información de alto nivel para permitir a la Comisión controlar la aplicación del Reglamento CPC y recuperar y compilar información estadística incorporada. Por esta razón, no debería ser necesario un acceso sistemático a todos los datos vinculados a los expedientes en las solicitudes de información y ejecución, incluso con fines de extracción de información estadística.

La nueva Decisión de aplicación del Reglamento CPC debería limitar específicamente el acceso de la Comisión a lo requerido por el Reglamento CPC y a lo estrictamente necesario para la realización de sus misiones. La arquitectura del SCPC debe concebirse en consecuencia.

El acceso de las autoridades competentes debería limitarse a sus necesidades de información. El SCPC permite actualmente a cada autoridad competente designar libremente a los destinatarios de los mensajes de alerta. Por tanto, no puede excluirse actualmente que una autoridad competente difunda alertas más ampliamente que lo que sería estrictamente necesario para las finalidades de la alerta, "solamente a efectos de información". Las autoridades competentes deben ser conscientes de que deben evaluar caso por caso la utilidad de estas transferencias a todos los destinatarios y no difundir información más ampliamente de lo que requiere una cooperación eficaz. Esta es otra cuestión que debe abordarse en las directrices SCPC y en la arquitectura del sistema.

Durante la preparación del presente dictamen, la DG SANCO indicó que prevé configurar el sistema de tal modo que la información de retorno contemplada en el artículo 8, apartado 2 y en el artículo 7, apartado 6, se envíe a todas las autoridades responsables de la aplicación de la legislación relativa a la Directiva sobre protección de los consumidores o al Reglamento en cuestión (por ejemplo, la Directiva sobre el comercio electrónico o sobre la utilización a tiempo parcial de bienes inmuebles - *time sharing*). El Grupo de Trabajo recomienda que la cuestión de los destinatarios y el contenido de la información de retorno se regulen en la nueva Decisión de aplicación del Reglamento CPC después de una atenta evaluación de la proporcionalidad del enfoque propuesto.

10.3. Exactitud. El artículo 6, apartado 1, letra d), de la Directiva 95/46/CE prevé que los datos personales deberán ser "exactos y, cuando sea necesario, actualizados" y que "deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados". El Reglamento (CE) n° 45/2001 prevé requisitos similares.

Tal como se expondrá en el punto 11 relativo al período de conservación, el SCPC tal como está diseñado actualmente no garantiza suficientemente que los datos potencialmente obsoletos no permanezcan en la base datos durante largos períodos, por ejemplo cuando los expedientes se perpetúan sin que se tome una medida al respecto o cuando la autoridad competente "se olvida" de informar a la Comisión sobre el cierre de un caso.

A este respecto, el Grupo de Trabajo considera que una revisión periódica de la información por parte de la autoridad competente que la haya proporcionado contribuiría a la exactitud de los datos almacenados en el SCPC. Con el fin de animar a los usuarios a efectuar esta revisión, la base de datos podría contener una función de recordatorio que alertaría a los usuarios periódicamente, por ejemplo cada seis meses o una vez el año, y les pediría que comprobasen la exactitud de la información que han introducido. Esta información se señalaría a continuación con una señal visible electrónica que indicaría que se ha efectuado la comprobación. También pueden añadirse comentarios relativos a la situación del caso.

11. PERIODO DE CONSERVACIÓN

El artículo 6, apartado 1, letra e), de la Directiva 95/46/CE prevé que los datos personales deben ser "conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente".

Los períodos de conservación descritos en el punto 6 *supra* plantean importantes cuestiones acerca de la protección de datos. En efecto, sin las protecciones y los límites necesarios, el SCPC corre el riesgo de convertirse en una base de datos gigantesca que contenga información obsoleta e inexacta, conservada durante largos períodos y utilizada por las autoridades competentes para obtener información con fines no especificados en el Reglamento CPC.

11.1. Período de cinco años para la conservación de los datos después de la ejecución. El Reglamento CPC prevé la obligación de conservar los datos relativos a infracciones durante cinco años en los casos en que se haya tomado una medida de ejecución, sin precisar no obstante la finalidad de conservar los datos durante un periodo tan largo. Este periodo de conservación obligatorio corre el riesgo de transformar el SCPC en una base de datos europea de empresas inscritas en una lista negra. Las personas físicas, comerciantes o proveedores, así como los directores, empleados u otras personas implicadas y que figuren en la base de datos podrían considerarse no dignas de confianza, únicamente en virtud de lo que podría ser a veces una simple asociación con una empresa infractora. No es posible saber si fue ésta la intención de los legisladores. Sin embargo, queda claro que tampoco hicieron explícita esta intención ni proporcionaron las garantías necesarias de protección de datos para garantizar que éstos puedan utilizarse con total seguridad para estos fines suplementarios.

El Grupo de Trabajo vuelve a lamentar que no se le haya consultado antes de adoptar el Reglamento CPC. De haberse hecho, habría expresado su seria preocupación en cuanto a la proporcionalidad del plazo de cinco años, y habría insistido también en que se precisase con claridad la finalidad de conservar los datos.

El Grupo de Trabajo mantiene estas preocupaciones y acogería con satisfacción una modificación del Reglamento CPC. No obstante, dado que debe emitir su dictamen a este respecto a posteriori, recomienda, como medida práctica, que hasta que los legisladores modifiquen el Reglamento CPC o especifiquen el objeto de tal período de conservación o bien lo supriman, la Comisión y las autoridades competente deberán interpretar la obligación de conservación durante cinco años de la manera más limitada posible y, al mismo tiempo, introducir una serie de garantías mínimas. Esto implica, entre otras cosas, una aclaración en un sentido favorable a la protección de datos y una respuesta a las siguientes cuestiones:

- ¿Cuál es la finalidad del período de cinco años para la conservación de los datos?

- ¿A qué datos se aplica este período?

- ¿Cuándo debe la información ser objeto de una notificación para su supresión?

Estas preguntas deberían encontrar una respuesta con el fin de garantizar que solamente se conserva la cantidad mínima de datos personales necesaria para una cooperación eficaz. Las respuestas deberían formalizarse en una nueva Decisión de aplicación del Reglamento CPC y también deberían introducirse modificaciones en la arquitectura de sistema del SCPC.

11.2. Casos "olvidados" o no notificados para su supresión. El Reglamento CPC y su Decisión de aplicación prevén la obligación de las autoridades competentes de informar a la Comisión cuando los casos se cierran o cuando ellas mismas determinan que una alerta es infundada. Sin embargo, deben resolverse varias lagunas:

- la autoridad competente puede simplemente decidir no cerrar un caso abierto aunque no se haya tomado ninguna medida de investigación y no haya aparecido ninguna información nueva durante un largo período de tiempo. En otras palabras: a veces hay casos que se eternizan;

- la autoridad competente puede cerrar un caso, pero "olvidar" notificar a la Comisión que los datos relativos a este caso deben suprimirse de la base de datos;

- la autoridad requerida puede acabar no adoptando una medida de ejecución, y por tanto no notificando a la Comisión, y no obstante la infracción puede cesar por otros motivos (por ejemplo, debido al inicio de una acción judicial por terceros).

Para abordar estas preocupaciones, el Grupo de Trabajo recomienda invertir la "lógica" de la conservación y la supresión de los datos: los casos deberán suponerse cerrados después de un periodo razonable a partir del envío de la solicitud de información o ejecución, y en ese momento los datos deberían suprimirse del SCPC, previa advertencia a las autoridades competentes interesadas, que deberían tener la posibilidad de confirmar que el caso sigue abierto. La ampliación del plazo de conservación debería concederse solamente por un período determinado, de modo que la necesidad de almacenamiento se revise periódicamente.

Si la autoridad competente no solicita una prórroga, toda la información vinculada al caso debería suprimirse.

Para garantizar que la información no se borre "por error", el sistema podría prever alertas repetidas y "períodos de gracia" razonables para manejar la situación cuando una autoridad competente no reaccione rápidamente. Durante la elaboración del presente dictamen, la DG SANCO explicó que ya está ocupada en poner a punto el envío de recordatorios a las autoridades competentes, cada 6 ó 12 meses, cuando alguno de sus casos parezca "dormido". El Grupo de Trabajo expresa su satisfacción por esta iniciativa y fomenta la continuación de estos planes con el fin de responder de una manera más amplia a la recomendación hecha en el presente dictamen.

11.3 Conservación de datos fuera del SCPC. Por último, el Grupo de Trabajo indica que, en este documento, no aborda la cuestión del periodo de tiempo durante el cual una autoridad competente puede conservar fuera del sistema los datos intercambiados a través del sistema, por ejemplo en un documento impreso adjunto al expediente correspondiente. Sin embargo, el Grupo de Trabajo llama la atención de las autoridades competentes y de la Comisión sobre el hecho de que la legislación y los principios de protección de datos se aplican de la misma manera al almacenamiento de información fuera del SCPC.

12. TRATAMIENTO DE DATOS SENSIBLES

12.1. Origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, pertenencia a sindicatos y salud o sexualidad. El artículo 8 de la Directiva 95/46/CE prohíbe el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. El artículo 10 del Reglamento (CE) n° 45/2001 contiene una prohibición similar.

Ningún dato de esta naturaleza se trata sistemáticamente en el SCPC, aunque ni el Reglamento CPC ni la Decisión que lo aplica prohíben específicamente este tratamiento, y es posible que estos datos puedan, en su caso, incluirse en la información intercambiada. Por ejemplo, en un documento adjunto como prueba de compra de determinados productos o servicios puede figurar información sensible sobre un cliente.

El Grupo de Trabajo recomienda que se modifique la Decisión de aplicación del Reglamento CPC para prohibir explícitamente el tratamiento de esta categoría especial de datos, permitiendo al mismo tiempo, si fuere necesario, algunas excepciones estrictamente definidas.

12.2. Datos relativos a infracciones, a supuestas infracciones y medidas de seguridad. El apartado 5 del artículo 8 de la Directiva 95/46/CE dispone que "el tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. […] Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos."

El SCPC incluye sistemáticamente datos relativos a infracciones o a supuestas infracciones, en particular actividades que infringen la legislación sobre protección de los consumidores. Puede tratarse tanto de infracciones administrativas como penales. Las sanciones administrativas, las condenas penales, las sentencias en asuntos civiles y las medidas de seguridad también podrán figurar en la base de datos.

El Reglamento CPC, que es directamente aplicable en los Estados miembros, autoriza el tratamiento de estos datos. El Grupo de Trabajo destaca no obstante que no debería considerarse que este Reglamento autoriza global e incondicionalmente este tratamiento. La utilización de los datos debe limitarse a fines específicos de asistencia mutua.

12.3. Número nacional de identificación. El apartado 7 del artículo 8 de la Directiva prevé que los Estados miembros "determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento". A su vez, el apartado 6 del artículo 10 del Reglamento prevé que "el Supervisor Europeo de Protección de Datos determinará las condiciones en las que podrá ser objeto de tratamiento un número personal o cualquier otro medio de identificación de aplicación general por parte de una institución o un organismo comunitario."

Ni el Reglamento CPC, ni la Decisión de aplicación de este Reglamento, ni el documento de debate de la Comisión sugieren que se utilicen sistemáticamente números nacionales de identificación en el SCPC. La Decisión, al especificar los distintos campos de datos que deben servir para identificar a un comerciante o a un proveedor, menciona otra información, como la dirección y los números de teléfono, pero no establece una entrada específica para los números nacionales de identificación. Dicho esto, no puede excluirse que un agente responsable de la ejecución de una autoridad competente no pueda incluir los números nacionales de identificación de determinadas personas, por ejemplo las personas físicas comerciantes o proveedores, directores o empleados, demandantes, testigos u otras partes involucradas.

Habida cuenta de la naturaleza sensible de los números nacionales de identificación, al menos en algunos Estados miembros, el Grupo de Trabajo recomienda que, a menos que la identificación sea estrictamente necesaria y no pueda ser efectuada de forma fiable por otros medios (por ejemplo, utilizando la dirección, la designación del empleo u otro identificador), debe evitarse utilizar estos números nacionales en el SCPC. En cualquier caso, de utilizarse estos números en estas circunstancias excepcionales, deberá tenerse en cuenta plenamente las posibles restricciones impuestas por las legislaciones nacionales sobre protección de datos en el momento de introducir o tratar estos datos.

13. EXENCIONES Y RESTRICCIONES

El apartado 4 del artículo 13 del Reglamento CPC prevé que, a efectos de la aplicación de este Reglamento, "los Estados miembros adoptarán las medidas legislativas necesarias para restringir los derechos y las obligaciones previstos en los artículos 10, 11 y 12 de la Directiva 95/46/CE en la medida que se requiera para salvaguardar los intereses contemplados en las letras d) y f) del apartado 1 del artículo 13 de dicha Directiva. La Comisión podrá restringir los derechos y las obligaciones previstos en el apartado 1 del artículo 4, el artículo 11, el apartado 1 del artículo 12, los artículos 13 a 17 y el apartado 1 del artículo 37 del Reglamento (CE) no 45/2001 cuando dicha restricción constituya una medida necesaria para salvaguardar

los intereses a que se hace referencia en las letras a) y e) del apartado 1 del artículo 20 de dicho Reglamento."

Esta disposición no sustituye al sistema heterogéneo preexistente, en el que las limitaciones a los derechos de las personas interesadas, en particular sus derechos en materia de información y de acceso, variaban de acuerdo con las distintas exenciones legislativas adoptadas en los Estados miembros. Esto puede ser comprensible a la luz de las diferencias que existen entre los Estados miembros en cuestiones que implican procedimientos judiciales, penales o administrativos y el acceso a los documentos relativos a estos procedimientos. No obstante, la falta de armonización a este respecto dificulta especialmente el cumplimiento de la normativa en materia de protección de datos y la cooperación entre los Estados miembros por lo que se refiere a las autorizaciones de acceso, tal como se mostrará en el punto 15. Con el fin de facilitar un entendimiento común y animar a los legisladores nacionales a elaborar una serie de principios comunes, el Grupo de Trabajo emite las recomendaciones que figuran más abajo.

13.1. Exenciones y restricciones que deben fijar los Estados miembros. El artículo 13, apartado 1, letra d) prevé que podrán establecerse limitaciones cuando tales limitaciones constituyan una medida necesaria para la salvaguardia de "la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas". El artículo 13, apartado 1, letra f) precisa por otro lado que la misma excepción se aplica a "una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública" con arreglo al artículo 13, apartado 1, letra d).
El Grupo de Trabajo recomienda que los Estados miembros, cuando adopten medidas destinadas a limitar los derechos y las obligaciones con arreglo a los artículos 10, 11 y 12 de la Directiva 95/46/CE, tengan en cuenta el hecho de que estas restricciones deben limitarse a lo estrictamente necesario para salvaguardar el interés mencionado en el artículo 13, apartado 1, letras d) y f), de la Directiva 95/46/CE.

En primer lugar, las limitaciones sólo deberían aplicarse respecto de los derechos a la información de los interesados con arreglo a los artículos 10 y 11 de la Directiva 95/46/CE o sus derechos de acceso, rectificación, supresión o bloqueo de conformidad con lo dispuesto en el artículo 12. No está permitida la limitación de ningún otro derecho contemplado en el artículo 13 de la Directiva 95/46/CE, en particular los principios relativos a la calidad de los datos o el requisito de notificación a las autoridades responsables de la protección de datos.

En segundo lugar, ni la Directiva 95/46/CE ni el Reglamento (CE) n° 45/2001 prevén una norma global y sistemática que prive de sus derechos de información y acceso a todas las personas interesadas cuyos datos puedan tratarse en relación con delitos penales e infracciones de la deontología de profesiones reguladas. La adopción de medidas restrictivas no debería ser arbitraria ni desproporcionada, ni tampoco limitar sistemáticamente el derecho de información de las personas interesadas ni su derecho de acceso a sus datos personales.

Las limitaciones sólo podrán estar permitidas si la divulgación de información a los interesados o el acceso de los mismos a los datos pudiera poner en peligro los fines de "la prevención, la investigación, la detección y la represión". En otros términos, recogiendo la terminología del artículo 13, apartado 3, del Reglamento CPC, las limitaciones sólo están permitidas si la concesión de derechos a los interesados pudiera poner en peligro "la finalidad de inspecciones o investigaciones".

Aunque una orientación legislativa general es bienvenida en los casos en los que sea posible, es necesario un análisis de los hechos caso por caso para determinar si se permite una limitación de los derechos de acceso a la información. Las directrices del SCPC mencionadas *supra* deberían contener más orientación a este respecto.

En tercer lugar, las excepciones a los derechos de protección de los datos sólo se aplican temporalmente, mientras sean necesarias para salvaguardar los fines de la "prevención, la investigación, la detección y la represión".

En cuarto lugar, las personas interesadas deben ser informadas de las principales razones en que se basa la limitación y de su derecho a recurrir ante las autoridades nacionales responsables de la protección de datos. La provisión de información puede diferirse mientras esta información prive a la limitación de sus efectos.

En cualquier caso, el Grupo de Trabajo recomienda que toda limitación figure claramente en las declaraciones de las distintas autoridades competentes relativas al derecho a la intimidad.

13.2. Exenciones y restricciones que debe fijar la Comisión. El Reglamento CPC prevé posibilidades de limitación similares para la Comisión por lo que se refiere a los derechos de las personas interesadas. Sin embargo, los derechos de la Comisión son más amplios que los de los Estados miembros. En particular, la Comisión puede limitar las disposiciones del Reglamento (CE) n° 45/2001 por lo que se refiere a la calidad de los datos, y puede conservar los datos de tráfico relativos a los usuarios al final de cada llamada o de cualquier otra conexión.
El Grupo de Trabajo destaca que todas las observaciones mencionadas anteriormente con respecto a las limitaciones que pueden ser aplicadas por las autoridades competentes en los Estados miembros se aplican también a la Comisión.

Además, al Grupo de Trabajo le preocupa la posibilidad que el Reglamento CPC confiere a la Comisión de limitar las disposiciones del Reglamento (CE) n° 45/2001 por lo que se refiere a i) la calidad de los datos y ii) la conservación de datos relativos al tráfico.

La posibilidad de limitar los principios fundamentales, como los principios relativos a la calidad de los datos, debe restringirse estrictamente a los casos en los que tal limitación resulte indispensable. En efecto, el Grupo de Trabajo no imagina una situación que justifique limitaciones en el contexto de la cooperación entre las autoridades responsables de la protección de los consumidores, por lo que se refiere por ejemplo a la publicidad engañosa, los viajes combinados o la utilización a tiempo parcial de bienes inmuebles, incluso cuando se produzcan actividades fraudulentas.

Por lo que se refiere a la posible conservación de datos sobre el tráfico por la Comisión, el Grupo de Trabajo no comprende con qué objetivo podría alegarse esta disposición, dado que todos los datos sobre el tráfico que figuran en el SCPC se refieren a intercambios de información entre autoridades competentes y que no hay razón alguna para que la Comisión conserve el contenido de estas comunicaciones más allá de lo permitido (por ejemplo, conservación durante seis meses para permitir la comprobación del uso autorizado). Mientras el contenido de los datos propiamente dicho figure en la base de datos, es legítimo almacenar algunos datos sobre el tráfico, tales como la "fecha de introducción" en el sistema. Una vez que el contenido de la comunicación se borra, por ejemplo cuando se retira una alerta, no es necesario conservar los datos sobre el tráfico.

14. INFORMACIÓN QUE DEBE PROPORCIONARSE A LA PERSONA INTERESADA

De conformidad con lo dispuesto en los artículos 10 y 11 de la Directiva 95/46/CE, los responsables del tratamiento deben informar a las personas interesadas del tratamiento de sus datos personales. El Reglamento (CE) n° 45/200 establece requisitos similares. Las personas físicas también deben ser informadas, entre otras cosas, de la finalidad del tratamiento, de los destinatarios de los datos y de sus derechos específicos como personas interesadas. El derecho de información es esencial en sí. Además, permite a las personas físicas ejercer otros derechos: si ignoran que se está tratando información que los concierne, no estarán en condiciones de ejercer otros derechos, como el derecho de acceso y rectificación.

Ni el Reglamento CPC, ni la Decisión de aplicación del Reglamento CPC, ni el documento de debate de la Comisión prevén disposiciones relativas a los derechos de información de las personas interesadas (excepto lo que figura en el punto 13 con respecto a las limitaciones). El Grupo de Trabajo recomienda la adopción de un enfoque por etapas.

14.1. Aviso general relativo al derecho a la intimidad en la página web del SCPC de la Comisión. En su página web dedicada al SCPC, la Comisión debería incluir un aviso general relativo al derecho a la intimidad que recoja todos los puntos requeridos con arreglo a los artículos 10 y 11 del Reglamento (CE) n° 45/2001. Este aviso también debería contener una descripción del SCPC y de los papeles de la Comisión y las autoridades competentes con un nivel de detalle al menos comparable a las explicaciones proporcionadas en el presente documento. El Grupo de Trabajo recomienda también que este aviso precise expresamente cómo pueden ejercer sus derechos de acceso las personas interesadas y cuáles son las restricciones impuestas a estos derechos, sin enumerar no obstante las distintas limitaciones específicas de los Estados miembros. La declaración relativa al derecho a la intimidad debe redactarse en un lenguaje claro y sencillo, accesible para las personas interesadas que no posean conocimientos en el ámbito de la protección de datos.

14.2. Aviso general relativo al derecho a la intimidad en las páginas web de las autoridades competentes. Las autoridades competentes deberían también incluir un aviso general relativo al derecho a la intimidad en su página web. A este respecto, el Grupo de Trabajo señala también que, además de las obligaciones en virtud de la Directiva 95/46/CE, el artículo 4, apartado 8, del Reglamento CPC prevé específicamente que "cada autoridad competente informará al público general sobre sus derechos y responsabilidades con arreglo al presente Reglamento". El aviso relativo al derecho a la intimidad debería incluir una referencia y un enlace al aviso de la Comisión a este respecto, así como otros detalles específicos de la autoridad o el Estado miembro en cuestión. Estos avisos deberán incluir, por ejemplo, las limitaciones nacionales a los derechos de acceso o de información. La difusión del aviso podrá estar coordinada por la oficina de enlace única entre las autoridades competentes en un país determinado.

14.3 Aviso dirigido directamente a las personas interesadas. A más tardar en el momento de la introducción de los datos personales, y a menos que pueda aplicarse una limitación (véase el punto 13), también deberá enviarse el aviso a las personas interesadas por otros medios distintos al aviso relativo al derecho a la intimidad en la página web. Esta comunicación podría hacerse incluyendo en toda la correspondencia que se intercambie con la

persona interesada (vendedor, director, demandante, testigo, etc.) una breve referencia al SCPC y un enlace hacia los avisos en Internet en materia de derecho a la intimidad.

Si la comunicación de estos avisos individuales resulta imposible o requiere esfuerzos desproporcionados (por ejemplo, si la autoridad competente no dispone de los datos de la persona interesada), puede omitirse tal comunicación. Tal como se indica en el punto 13, el suministro de información también puede diferirse si los derechos de información se ven temporalmente limitados.

15. DERECHO DE ACCESO DE LAS PERSONAS INTERESADAS A LOS DATOS

El artículo 12, letra a), de la Directiva 95/46/CE establece que los interesados tendrán el derecho de obtener del responsable del tratamiento: i) la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios, y ii) la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos.

Además, la letra b) del artículo 12 establece que los interesados tendrán el derecho de obtener del responsable del tratamiento, en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva 95/46/CE, en particular a causa del carácter incompleto o inexacto de los datos. El Reglamento (CE) n° 45/2001 contiene disposiciones similares.

Ni el Reglamento CPC, ni la Decisión de aplicación del Reglamento CPC, ni el documento de debate de la Comisión contienen disposiciones relativas a los derechos de acceso de las personas interesadas. Se trata en efecto de una cuestión compleja, habida cuenta de los distintos actores implicados en las actividades de tratamiento de los datos.

Varias autoridades competentes, así como la Comisión, tienen acceso a determinados datos personales introducidos en el sistema. A menudo, varios intervinientes tienen acceso a la misma información. En general, por ejemplo, dos autoridades, o a veces más, tienen acceso a las solicitudes de información y ejecución. Algunas autoridades, así como la Comisión, pueden tener acceso a la información sobre alertas. Las personas interesadas pueden dirigirse a varias autoridades para pedir sus derechos de acceso.

La situación es tanto más difícil cuanto que las normas relativas a las limitaciones de acceso varían de un Estado miembro a otro, como se ha visto en el punto 13. Teniendo en cuenta que existen distintas limitaciones a los derechos de acceso en los Estados miembros, es posible que un Estado miembro permita acceder a unos datos, mientras que otro no lo haga. Por tanto, es indispensable que las autoridades competentes cooperen respecto de cada solicitud de acceso que reciban.

Las recomendaciones que el Grupo de Trabajo formula a continuación describen dos situaciones, que requieren medidas de coordinación específicas con el fin de garantizar la conformidad: i) se solicita información a una autoridad competente, pero el hecho de permitir el acceso a estos datos puede influir en las actividades de investigación o ejecución de otra autoridad; y ii) las personas interesadas envían sus solicitudes de acceso a la Comisión.

15.1. Coordinación entre autoridades competentes. El Grupo de Trabajo recomienda que, si la concesión de acceso a datos personales puede influir en el procedimiento de investigación o de ejecución realizado por otras autoridades competentes, la autoridad competente a la que se haya presentado la solicitud de acceso deberá solicitar la opinión de estas otras autoridades antes conceder el acceso.
El acceso deberá concederse únicamente si las otras autoridades competentes interesadas han tenido la ocasión de comunicar sus posiciones y se han tenido en cuenta las posibles objeciones a la concesión del acceso basadas en exenciones en virtud de su legislación nacional en materia de protección de datos. Si las autoridades no responden en un plazo razonable o no plantean objeciones, la autoridad a la que se haya presentado la solicitud de acceso podrá decidir en función de su propia legislación nacional si se aplica una exención o si puede concederse el acceso. Si las autoridades no están de acuerdo sobre la concesión del acceso, la autoridad que haya proporcionado la información deberá ser la que fije finalmente los criterios de acceso.

Un mecanismo de cooperación similar debería aplicarse a la rectificación, a la supresión o al bloqueo de los datos.

El Grupo de Trabajo destaca sin embargo que este procedimiento de coordinación no debería utilizarse para denegar arbitrariamente el acceso a las personas interesadas ni para prolongar artificialmente el plazo necesario para la concesión del derecho de acceso. Además, la denegación de este derecho debe justificarse claramente, y la persona interesada debe ser informada de que, en su caso, puede dirigirse a otra autoridad competente para obtener este derecho de acceso.

15.2. Coordinación entre la Comisión y las autoridades competentes. Es posible que las personas interesadas envíen sus solicitudes de acceso a la Comisión.
A este respecto, conviene en primer lugar destacar que la Comisión sólo puede proporcionar acceso a los datos a los que ella misma tiene acceso legítimo. No tiene por tanto obligación de proporcionar acceso a solicitudes de información, a solicitudes de ejecución ni a comunicaciones relacionadas. En estos casos, deberá dirigir a las personas interesadas a las autoridades que tienen acceso a la información.

La situación es diferente respecto a la información a la que la Comisión tiene acceso legítimo, por ejemplo la información de alerta o la información de retorno. A este respecto, el Grupo de Trabajo recomienda que, cuando la Comisión reciba una solicitud de acceso, solicite la opinión de la autoridad competente que haya proporcionado la información en primer lugar. Entonces deberá concederse el acceso solamente si el socio que aporta la información ha tenido la ocasión de comunicar su posición y si se ha examinado cualquier objeción a la concesión del acceso basada en una excepción específica en virtud de su legislación nacional sobre protección de datos. Si el socio que aporta la información no responde en un plazo razonable o si no plantea objeciones, la Comisión puede decidir sobre la base del Reglamento (CE) n° 45/2001 si se aplica una excepción o si puede concederse el acceso.

Además de ponerse en contacto con la autoridad competente que haya proporcionado la información, la Comisión debe también dar a todas las demás autoridades competentes cuyas actividades de investigación o ejecución podrían verse en peligro la oportunidad de expresar sus preocupaciones. Sin embargo, si las autoridades no están de acuerdo sobre la concesión del acceso, la autoridad que haya proporcionado la información deberá ser la que fije finalmente los criterios de acceso.

Un mecanismo similar de cooperación debería aplicarse a la rectificación, la supresión o el bloqueo de los datos.

16. MEDIDAS DE RECURSO

Sin perjuicio de la disponibilidad de recursos administrativos ante las autoridades nacionales de protección de datos o el SEPD, el artículo 22 de la Directiva 95/46/CE exige a los Estados miembros que prevean que toda persona disponga de un recurso jurisdiccional en caso de violación de los derechos que le garantizan las disposiciones nacionales aplicables sobre protección de datos. El artículo 23, en particular, exige a los Estados miembros que dispongan que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

Según el análisis del Grupo de Trabajo relativo a los actores del SCPC, tal como se indica en el punto 8, la Comisión, las oficinas de enlace únicas y las autoridades competentes se considerarán responsables del tratamiento por lo que respecta a sus propias tareas y responsabilidades, y responderán por lo que respecta a sus propias funciones, tareas y responsabilidades.

17. SEGURIDAD

Con arreglo al artículo 22 del Reglamento (CE) n° 45/2001, el responsable del tratamiento pondrá en práctica las medidas de carácter técnico y organizativo adecuadas para garantizar un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse. La Directiva 95/46/CE prevé medidas de seguridad similares.

La Comisión, que es el operador del SCPC y responsable del tratamiento designada en virtud del Reglamento CPC, está sujeta a las disposiciones del Reglamento (CE) n° 45/2001.

Considerando, por una parte, que las legislaciones nacionales relativas a la protección de datos están en gran parte armonizadas sobre la base de la Directiva 95/46/CE y, por otra parte, que tal armonización no está completa y que existen algunas diferencias entre los Estados miembros en cuanto al nivel de seguridad aceptable, el Grupo de Trabajo recomienda que las disposiciones del Reglamento (CE) n° 45/2001 en materia de seguridad se interpreten de acuerdo con las mejores prácticas en los Estados miembros. Se debería también fomentar que los Estados miembros aumenten la seguridad del acceso por parte de las autoridades competentes.

Si se produce una violación de la seguridad o la confidencialidad, las personas interesadas podrían quejarse al SEPD, que tiene poderes de supervisión sobre la Comisión, de acuerdo con las disposiciones del Reglamento (CE) n° 45/2001. El SEPD puede también realizar por iniciativa propia una inspección de la seguridad o una auditoría de la base de datos. Estas operaciones pueden tener lugar tanto en el marco del procedimiento de control previo contemplado en el punto 18 *infra* como fuera del mismo.

18. NOTIFICACIÓN Y CONTROL PREVIO

18.1. Autoridades nacionales responsables de la protección de datos. En aplicación de los artículos 18, 19 y 20 de la Directiva 95/46/CE, las autoridades competentes de varios Estados miembros deben notificar sus operaciones de tratamiento en el marco del SCPC a las autoridades nacionales responsables de la protección de datos. En algunos Estados miembros, es posible que las operaciones de tratamiento deban ser controladas de antemano por estas autoridades.

En los Estados miembros que prevén tal procedimiento, las operaciones de tratamiento están sometidas al control previo por parte de las autoridades nacionales, puesto que pueden presentar riesgos específicos respecto a los derechos y libertades de las personas en cuestión. Este el caso, por ejemplo, cuando la legislación nacional exige que el tratamiento de datos relativos a infracciones penales o presuntas infracciones penales sea objeto de un control previo. En cuanto a saber si estas operaciones de tratamiento están sujetas al requisito del control previo, esto depende de la legislación nacional y de la práctica de la autoridad nacional responsable de la protección de datos.

18.2. Control previo por el SEPD. La información intercambiada contiene datos personales relativos a delitos, presuntos delitos, condenas penales, y también posiblemente medidas de seguridad. Habida cuenta de la naturaleza de los datos y del papel de la Comisión en el caso presente, la base de datos debería someterse al control previo con arreglo al artículo 27, apartado 2, letra a), del Reglamento (CE) n° 45/2001.

El tratamiento también está sujeto al artículo 27, apartado 2, letra b), de dicho Reglamento, que prevé que los tratamientos "destinados a evaluar aspectos de la personalidad del interesado, como su competencia, rendimiento o conducta" están sujetos al control previo del SEPD. En efecto, los datos contenidos en el SCPC podrán utilizarse para evaluar el comportamiento de las personas físicas (comerciantes, directores, y quizá también miembros del personal u otros) que supuestamente están implicados en infracciones, con el fin de determinar las medidas adecuadas que deben adoptarse (medidas de investigación o ejecución).

El control previo es tanto más necesario cuanto que: i) los detalles de la base de datos no se fijaron en un Reglamento o una Directiva de alto nivel del Parlamento y el Consejo; ii) el SEPD no aconsejó a los legisladores durante el proceso legislativo; y iii) se ha designado a la Comisión responsable del tratamiento en virtud del Reglamento CPC.

Como el sistema ya está en funcionamiento, el SEPD deberá realizar el examen del control previo a posteriori.

18.3. Coordinación de los procedimientos de notificación y control previo. Habida cuenta de que las autoridades competentes, así como la Comisión, son responsables del tratamiento, y que en algunos Estados miembros existen varias autoridades competentes, el Grupo de Trabajo recomienda que los procedimientos de control previo se coordinen entre las autoridades nacionales responsables de la protección de datos y el SEPD, para poder desarrollar un enfoque coherente.

19. TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES

El artículo 14, apartado 2, del Reglamento CPC prevé que la información comunicada con arreglo al Reglamento CPC "podrá también transmitir[se] a la autoridad de un tercer país en el marco de un acuerdo bilateral de asistencia mutua con dicho país, siempre que la autoridad competente que envió inicialmente la información dé su consentimiento y de conformidad con la legislación comunitaria en materia de protección de las personas respecto del tratamiento de datos personales."

De conformidad con lo dispuesto en el artículo 25 de la Directiva 95/46/CE, las transferencias a un país tercero sólo pueden tener lugar si el país tercero en cuestión garantiza un nivel de protección adecuado. El artículo 26 de la Directiva 95/46/CE prevé algunas excepciones a este principio. Entre éstas figura la del artículo 26, apartado 1, letra d), que prevé que "la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante". El apartado 2 del artículo 26 prevé por otro lado que los Estados miembros podrán autorizar transferencias cuando el responsable del tratamiento ofrezca garantías suficientes, en particular mediante cláusulas contractuales apropiadas.

La ejecución y la interpretación de estas disposiciones pueden variar de un Estado miembro a otro. Por tanto, el Grupo de Trabajo acoge con satisfacción que el Reglamento CPC someta expresamente toda transferencia de datos hacia un tercer país al consentimiento de la autoridad competente que haya proporcionado la información inicialmente.

El Grupo de Trabajo recomienda por otro lado a los Estados miembros que velen por que los acuerdos de asistencia bilateral con terceros países se revisen con el fin de prever garantías adecuadas relativas a la protección de datos.

20. CONCLUSIONES

En conclusión, el Grupo de Trabajo se felicita por que el SCPC disponga de una base jurídica adecuada, se establezca para fines legítimos y pueda servir de instrumento para la protección de datos con el fin de contribuir a la cooperación entre las autoridades competentes y la Comisión, siempre que se tengan en cuenta plenamente las recomendaciones del Grupo de Trabajo.

Dicho esto, el Grupo de Trabajo reitera su pesar por no haber sido consultado en una fase anterior del procedimiento, antes de la adopción del Reglamento CPC, de la Decisión de aplicación de este Reglamento y del inicio del funcionamiento del SCPC.

De momento, sobre la base del texto actual del Reglamento CPC, el Grupo de Trabajo recomienda varias medidas que deberían ser adoptadas por la Comisión y las autoridades competentes para mejorar la conformidad con las disposiciones en materia de protección de datos. En algunos casos, la adopción de medidas puede exigir el recurso al procedimiento reglamentario y la emisión de una nueva Decisión de aplicación del Reglamento CPC con la

ayuda del Comité. Otras recomendaciones podrían aplicarse a un nivel más operativo, por la Comisión, a través de las directrices del SCPC y mediante la formación impartida a los agentes responsables de la ejecución, así como mediante modificaciones de la arquitectura del SCPC.

El Grupo de Trabajo destaca también que, en el marco del funcionamiento y la utilización del sistema, las autoridades competentes y la Comisión deben ser conscientes de la naturaleza especial de su papel de control, así como de la diversidad de las legislaciones aplicables en materia de protección de datos y la diversidad de las autoridades de control. Deben esforzarse en cooperar plenamente para garantizar el respeto de las legislaciones sobre protección de datos.

El Grupo de Trabajo recomienda en particular lo siguiente:

- Los agentes responsables de la ejecución que trabajan para las autoridades competentes deberían evaluar caso por caso la conformidad con los principios de protección de datos.

  - Para ayudar a la toma de decisiones, la Comisión debería elaborar y difundir directrices para el SCPC.

  - Siempre que sea posible, las características técnicas del SCPC deberían adaptarse con el fin de incluir recordatorios y otras medidas técnicas para contribuir a la conformidad con los principios de la protección de datos.

  - Los principios de la protección de datos deberían integrarse en la formación de los agentes responsables de la ejecución.

- Los fines para los que las autoridades competentes y la Comisión pueden tener acceso a la base de datos deberían limitarse y especificarse claramente. La Comisión no debería tener acceso a las solicitudes de información y ejecución (excepto la información de retorno importante), y su acceso a la información registrada como confidencial debe también limitarse a los casos para los que tal acceso sea necesario y proporcionado.

- Los agentes responsables de la ejecución deberían limitar la introducción de datos personales a lo estrictamente necesario a efectos de la eficacia de la cooperación. Esto se aplica en particular a la información relativa a los directores, así como a todos los demás datos personales que figuran en los documentos adjuntos y en los breves resúmenes.

- Los agentes responsables de la ejecución deberían también abstenerse de difundir las alertas o las solicitudes de asistencia mutua más ampliamente de lo que sea estrictamente necesario.

- Deberían adoptarse medidas con el fin de comprobar periódicamente la exactitud de los datos introducidos en la base de datos.

- Los agentes responsables de la ejecución deberían evaluar periódicamente la necesidad de conservar la información. La lógica de la conservación y la supresión de

los datos debería invertirse: tras un recordatorio (o eventualmente recordatorios repetidos y períodos de gracia razonables), los datos deberían suprimirse automáticamente, salvo si las autoridades competentes confirman que aún no han cerrado el caso.

- Las personas interesadas deben ser informadas de que sus datos se han introducido en el SCPC, mediante un enfoque por etapas, que incluye avisos en la página web y también información comunicada directamente a los interesados. Este derecho no debería limitarse sistemáticamente, ya que las limitaciones a un derecho fundamental no pueden aplicarse sistemáticamente. Lo mismo sucede con el derecho de acceso. Debe establecerse un mecanismo de cooperación eficaz para proporcionar acceso a las personas interesadas.

- Deberían adoptarse medidas de seguridad de acuerdo con las mejores prácticas en los Estados miembros.

- El SCPC debe estar sujeto al control previo del SEPD, así como a las autoridades responsables de la protección de datos en algunos Estados miembros. Deberá informarse a otras autoridades nacionales responsables de la protección de datos. Los procedimientos de control previo deben coordinarse.

Hecho en Bruselas, el 21 de septiembre de 2007

Por el Grupo de Trabajo

El Presidente
Peter Schaar