Resumen ejecutivo del dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación Conjunta de la Comisión Europea y de la Alta Representante para la Unión Europea para Asuntos Exteriores y Política de Seguridad «Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro», y la propuesta de la Comisión de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad en las redes y de la información en la Unión

(El texto completo del presente dictamen puede encontrarse en inglés, francés y alemán en el sitio web del SEPD http://www.edps.europa.eu)

(2014/C 32/10)

1. **Introducción**

1.1. *Consulta al Supervisor Europeo de Protección de Datos*

1. El 7 de febrero de 2013, la Comisión y la Alta Representante para la Unión Europea para Asuntos Exteriores y Política de Seguridad adoptaron la Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro» [1] (en adelante, la «Comunicación Conjunta», «la Estrategia de ciberseguridad» o la «Estrategia»).

2. En la misma fecha, la Comisión adoptó una propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión [2] (en adelante, «la propuesta de Directiva» o «la propuesta»). Dicha propuesta fue trasladada para consulta al SEPD el 7 de febrero de 2013.

3. Antes de que fueran adoptadas la Comunicación Conjunta y la propuesta, el SEPD pudo proporcionar observaciones informales a la Comisión. El SEPD recibe con agrado que la Comunicación Conjunta y la propuesta hayan tenido en cuenta algunas de sus observaciones.

4. **Conclusiones**

74. El SEPD recibe con agrado que la Comisión y la Alta Representante para la Unión Europea para Asuntos Exteriores y Política de Seguridad hayan presentado una Estrategia de ciberseguridad global que se complementa con una propuesta de Directiva relativa a medidas para garantizar un elevado nivel común de seguridad y de la información (SRI) en la Unión. La Estrategia complementa las intervenciones que ya han sido desarrolladas por la UE en el campo de la SRI.

75. El SEPD recibe con satisfacción que la Estrategia exceda el enfoque tradicional de oposición entre la seguridad y la intimidad, proporcionando el reconocimiento explícito de la intimidad y la protección de datos como valores esenciales que deben guiar la política de ciberseguridad tanto en la UE como internacionalmente. El SEPD señala que la Estrategia de ciberseguridad y la propuesta de Directiva sobre SRI pueden jugar un papel fundamental contribuyendo a garantizar la protección de los derechos de los interesados a la intimidad y la protección de datos en el entorno en línea. Al mismo tiempo, debe garantizarse que no conducen a medidas que pudieran plantear interferencias ilícitas con los derechos de los interesados a la intimidad y la protección de datos.

76. El SEPD recibe asimismo con agrado que se haga mención a la protección de datos en diversas partes de la Estrategia, así como que se haya tenido en cuenta en la propuesta de Directiva sobre SRI. Sin embargo, lamenta que tanto la Estrategia como la propuesta de Directiva no subrayen mejor la contribución que realizan a la legislación en materia de protección de datos existente y futura en la seguridad y no sean capaces de asegurar que las obligaciones resultantes de la propuesta de Directiva u otros elementos de la Estrategia sean complementarios con las obligaciones de protección de datos, así como que no se solapen o contradigan entre sí.

77. Asimismo, el SEPD señala que debido a la falta de consideración y teniendo plenamente en cuenta el resto de iniciativas paralelas de la Comisión y los procedimientos legislativos en curso, como la reforma de la protección de datos y la propuesta de Reglamento relativo a la identificación electrónica y los servicios de confianza, la Estrategia de ciberseguridad no ofrece una visión holística y realmente global de ciberseguridad en la UE y corre el riesgo de perpetuar un enfoque fragmentado y compartimentado. El SEPD señala

[1] JOIN(2013) 1 final.
[2] COM(2013) 48 final.

asimismo que la propuesta de Directiva sobre SRI no permite aún tener un enfoque global de la seguridad en la UE y que la obligación establecida en la legislación en materia de protección de datos probablemente constituye la red y la obligación de seguridad más generales con arreglo a la legislación europea.

78. El SEPD también lamenta que tampoco se ha considerado de forma adecuada el importante papel de las autoridades encargadas de la protección de los datos tanto en la aplicación y la observancia de las obligaciones de seguridad como en la mejora de la ciberseguridad.

79. Respecto de la Estrategia de ciberseguridad, el SEPD subraya que:

— una definición clara de los términos «ciberresiliencia», «ciberdelincuencia» y «ciberdefensa» resulta especialmente importante dado que estos términos se utilizan para justificar determinadas medidas especiales que podrían interferir con los derechos fundamentales, incluidos los derechos a la intimidad y la protección de datos. Sin embargo, las definiciones de «ciberdelincuencia» recogidas en la Estrategia y en el Convenio de ciberdelincuencia siguen siendo muy amplias. Sería aconsejable contar con una definición *restrictiva* de la «ciberdelincuencia» en lugar de una definición global,

— la legislación en materia de protección de datos debe aplicarse a todas las intervenciones de la Estrategia cuando afecten a medidas que impliquen el tratamiento de datos personales. Aunque la legislación en materia de protección de datos no se menciona de forma específica en las secciones relativas a la ciberdelincuencia y la ciberdefensa, el SEPD subraya que muchas de las acciones planificadas en dichos campos podrían implicar el tratamiento de datos personales y podrían, por tanto, entrar dentro del ámbito de aplicación de la legislación de protección de datos aplicable. Señala asimismo que muchas intervenciones consisten en el establecimiento de mecanismos de coordinación, que exigirán la aplicación de las garantías de protección de datos adecuadas, respecto de las disposiciones de intercambio de los datos personales,

— las autoridades encargadas de la protección de datos juegan un papel importante en el contexto de la ciberseguridad. Como guardianes de la intimidad y de los derechos de protección de datos de los interesados, las autoridades encargadas de la protección de datos se implican activamente en la protección de sus datos personales, tanto fuera de línea como en línea. Por lo tanto, deben participar de manera adecuada, en su calidad de organismos de supervisión, en relación con las medidas de ejecución que implican el tratamiento de datos personales (como el lanzamiento del proyecto piloto de la UE de lucha contra los botnets y el malware). Otros actores en el campo de la ciberseguridad también deben cooperar con ellas en el ejercicio de sus funciones, por ejemplo, en el intercambio de sus mejores prácticas y las acciones de sensibilización. El SEPD y las autoridades nacionales encargadas de la protección de datos también deberán implicarse de forma adecuada en la conferencia de alto nivel que se celebrará en 2014 para evaluar la evolución de la ejecución de la Estrategia.

80. Respecto de la propuesta de Directiva sobre SRI, el SEPD recomienda a los legisladores:

— ofrecer una mayor claridad y certeza en el artículo 3, apartado 8, sobre la definición de los operadores del mercado que entran dentro del ámbito de aplicación de la propuesta, y establecer una lista exhaustiva que incluya a todas las partes implicadas, para garantizar un enfoque integrado y completamente armonizado de la seguridad dentro de la UE,

— aclarar en el artículo 1, apartado 2, letra c) que la propuesta de Directiva es aplicable a las instituciones y organismos de la UE, así como incluir una referencia al Reglamento (CE) nº 45/2001 en el artículo 1, apartado 5 de la propuesta,

— reconocerle un papel más horizontal a esta propuesta respecto de la seguridad, indicando de forma explícita en el artículo 1 que dicho artículo se aplicará sin perjuicio de la existencia de normas más pormenorizadas existentes o futuras en ámbitos específicos (como las que serán establecidas por proveedores de servicios de confianza en la propuesta de Reglamento relativo a la identificación electrónica),

— añadir un considerando que explique la necesidad de incluir la protección mediante el diseño y por defecto desde una fase temprana del diseño de los mecanismos establecidos en la propuesta y a lo largo de todo el ciclo de vida de los procesos, procedimientos, organizaciones, técnicas e infraestructuras implicadas, teniendo en cuenta la propuesta de Reglamento de protección de datos,

— aclarar las definiciones de «redes y sistemas de información» en el artículo 3, apartado 1 y de «incidente» del apartado 4 del mismo artículo, y sustituir en el artículo 5, apartado 2, la obligación de establecer un «plan de evaluación del riesgo» por «establecer y mantener un marco de gestión de riesgos»,

— especificar en el artículo 1, apartado 6, que el tratamiento de los datos personales estaría justificado con arreglo a lo dispuesto en el artículo 7, letra e) de la Directiva 95/46/CE en la medida en que sea necesario cumplir los objetivos de interés público que persigue la propuesta de Directiva. Sin embargo, debe garantizarse el debido respeto de los principios de necesidad y de proporcionalidad, de forma que sólo se traten los datos estrictamente necesarios para el fin para el que fueron obtenidos,

— establecer en el artículo 14 las circunstancias en que resulta necesaria una notificación, así como el contenido y el formato de la notificación, incluidos los tipos de datos personales que deben notificarse y si, y en qué medida, la notificación y sus documentos justificativos incluirán los pormenores de los datos personales afectados por un incidente de seguridad específico (como las direcciones IP). Debe tenerse en cuenta el hecho de que debe permitirse a las autoridades competentes de la SRI obtener y tratar datos personales en el marco de un incidente de seguridad sólo cuando resulte estrictamente necesario. Deben establecerse asimismo las garantías adecuadas en la propuesta para garantizar la adecuada protección de los datos tratados por las autoridades competentes de la SRI,

— aclarar en el artículo 14 que las notificaciones de un incidente con arreglo al artículo 14, apartado 2, deben aplicarse sin perjuicio de las obligaciones de notificación de las violaciones de datos de acuerdo con lo dispuesto en la legislación en materia de protección de datos. Deben establecerse en la propuesta los principales aspectos del procedimiento para la cooperación de las autoridades competentes de la SRI con las autoridades nacionales encargadas de la protección de datos en que el incidente de seguridad implica una violación de los datos personales,

— modificar el artículo 14, apartado 8, para que la exclusión de las microempresas del alcance de la notificación no sea aplicable a aquellos operadores que juegan un papel crucial en la prestación de los servicios de la sociedad de la información, por ejemplo, a la luz de la naturaleza de la información que tratan (p. ej., datos biométricos o datos sensibles),

— añadir disposiciones en la propuesta que regulen el intercambio ulterior de datos personales por parte de las autoridades competentes de la SRI con otros destinatarios, para garantizar que i) los datos personales sólo se difundirán a los destinatarios cuyo tratamiento sea necesario para el ejercicio de sus funciones de acuerdo con una base jurídica adecuada y ii) dicha información se limita a lo que resulta necesario para ejercer sus funciones. Debe prestarse atención a que el modo en que las entidades facilitan datos a la red de intercambio de información garantice el cumplimiento del principio de limitación a una finalidad,

— especificar el plazo de conservación de los datos personales a los efectos establecidos en la propuesta de Directiva, en particular respecto de la conservación por parte de las autoridades competentes de la SRI y dentro de la infraestructura segura de la red de cooperación,

— recordar a las autoridades competentes de la SRI su deber de proporcionar a los interesados la información adecuada sobre el tratamiento de datos personales, por ejemplo, colgando una política de intimidad en su página web,

— añadir una disposición relativa al nivel de seguridad que deben cumplir las autoridades competentes de la SRI por lo que se refiere a la información recogida, tratada e intercambiada. Debe incluirse específicamente una referencia a los requisitos de seguridad del artículo 17 de la Directiva 95/46/CE, respecto de la protección de los datos personales por parte de las autoridades competentes de la SRI,

— aclarar en el artículo 9, apartado 2, que los criterios para la participación de los Estados miembros en el sistema seguro de intercambio de información debe garantizar que existe un alto nivel de seguridad y de resiliencia por parte de todos los participantes en los sistemas de intercambio de seguridad en todas las fases del tratamiento. Estos criterios deben incluir las medidas de confidencialidad y de seguridad adecuadas de conformidad con los artículos 16 y 17 de la Directiva 95/46/CE y los artículos 21 y 22 del Reglamento (CE) nº 45/2001. La Comisión debe queda expresamente obligada por estos criterios por su participación como responsable del tratamiento en el sistema seguro de intercambio de información,

— añadir en el artículo 9 una descripción de las funciones y responsabilidades de la Comisión y de los Estados miembros en el establecimiento, funcionamiento y mantenimiento del sistema seguro de intercambio de información, y establecer que el diseño del sistema debe establecerse de acuerdo con los principios de protección de datos mediante el diseño y por defecto y de la seguridad mediante el diseño, y

— añadir en el artículo 13 que todas las transferencias de datos personales a los destinatarios ubicados en países de fuera de la UE deben realizarse de conformidad con los artículos 25 y 26 de la Directiva 95/46/CE y el artículo 9 del Reglamento (CE) nº 45/2001.

Hecho en Bruselas, el 14 de junio de 2013.

Peter HUSTINX

Supervisor Europeo de Protección de Datos