SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Resumen ejecutivo del Dictamen del Supervisor Europeo de Protección de Datos relativo a la Comunicación de la Comisión al Parlamento Europeo y al Consejo «Restablecer la confianza en los flujos de datos entre la UE y EE. UU.» y relativo a la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE

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

(2014/C 116/04)

I. Introducción

I.1. *Consulta al Supervisor Europeo de Protección de Datos*

1. El 27 de noviembre de 2013, la Comisión adoptó la Comunicación de la Comisión al Parlamento Europeo y al Consejo «Restablecer la confianza en los flujos de datos entre la UE y EE. UU.» ([1]) (en adelante, «la Comunicación sobre el restablecimiento de la confianza»). Dicha Comunicación fue acompañada de un informe relativo a las conclusiones de los copresidentes de la UE del grupo de trabajo *ad hoc* UE-EE. UU. sobre protección de datos (en adelante, «el informe» y «el grupo de trabajo»).

2. Ese mismo día, la Comisión adoptó la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE ([2]) (en adelante, «la Comunicación sobre el puerto seguro»).

3. El SEPD recibe con agrado haber tenido la posibilidad de formular observaciones informales a la Comisión antes de la adopción de los documentos citados anteriormente. Dichos documentos fueron adoptados por la Comisión como consecuencia de las revelaciones sobre los programas de vigilancia realizados por los servicios de inteligencia de los EE. UU. Considerando el impacto que estos programas de vigilancia tienen sobre los derechos de privacidad y de protección de los datos personales de las personas físicas en la UE, el SEPD ha decidido adoptar el presente Dictamen por iniciativa propia.

I.2. *Objetivo y ámbito de aplicación de los documentos de la Comisión*

a) La Comunicación sobre el restablecimiento de la confianza y el informe

4. La Comunicación propone una forma eficaz siguiendo las revelaciones sobre los programas estadounidenses a gran escala de recopilación de información de inteligencia (en adelante, «los programas») y su impacto en la confianza entre la UE y EE. UU. No hace referencia a las revelaciones sobre la realización de actividades similares o la colaboración de EE. UU. con los Estados miembros de la UE o con terceros países.

5. El informe examina las conclusiones de los copresidentes de la UE del grupo de trabajo *ad hoc* UE-EE. UU. sobre protección de datos, que fue creado tras la reunión del Coreper de 18 de julio de 2013 para determinar los hechos sobre los programas y su impacto sobre los derechos fundamentales en la UE y los datos personales de los ciudadanos europeos. Analiza el marco jurídico estadounidense ([3]), el modo de recogida y el tratamiento ulterior de los datos ([4]) y los mecanismos de control y de recurso existentes.

([1]) COM(2013) 846 final.

([2]) COM(2013) 847 final.

([3]) En particular, la Constitución, tal como ha interpretado el Tribunal Supremo de los Estados Unidos; el artículo 702 de la *Foreign Intelligence Surveillance Act* (Ley de vigilancia de inteligencia exterior) de 1978 (FISA, por sus siglas en inglés) (modificada por la *FISA Amendments Act* de 2008 (Ley modificativa d la ley de vigilancia a la inteligencia exterior), 50 *U.S.C* (Título 50 del Código de EE. UU.) § 1881a); y el artículo 215 de la *USA PATRIOT Act* (Ley patriota de los EE. UU.) de 2001 (también modificado por la Ley FISA, 50 U.S.C. de 1861) y la Orden ejecutiva 12333.

([4]) Sobre la base de la información proporcionada por EE. UU. en el grupo de trabajo y en los documentos desclasificados, incluidos los dictámenes del *Foreign Intelligence Surveillance Court* (Tribunal de Vigilancia de Inteligencia Exterior, en adelante «FISC», por sus siglas en inglés) y en los documentos públicamente disponibles como las Directrices del Fiscal General para las operaciones nacionales del FBI.

6. El informe menciona una «segunda vía» que también fue establecida durante la reunión del Coreper de 18 de julio de 2013. Establece que, con arreglo a dicha «segunda vía» las instituciones europeas podrán formular preguntas a las autoridades estadounidenses relacionadas con la supuesta vigilancia de las misiones diplomáticas y las instituciones de la UE, mientras que los Estados miembros podrán debatir con las autoridades estadounidenses, de forma bilateral, las cuestiones relacionadas con su seguridad nacional.

7. El informe también establece que dicha división limita en cierta medida el debate en el grupo de trabajo y la información que este facilita. El SEPD no ha recibido ninguna información sobre dicha «segunda vía» ni sobre la creación de un grupo de trabajo paralelo en este sentido. En consecuencia, se pide a la Comisión que informe al SEPD sobre las conclusiones de la «segunda vía», en particular respecto de la supuesta vigilancia de las misiones diplomáticas y de las instituciones de la UE.

b) La Comunicación sobre el puerto seguro

8. La Comunicación sobre el puerto seguro analiza el funcionamiento del puerto seguro, identifica las deficiencias y propone posibles mejoras. Reconoce la creciente cantidad de datos transmitidos entre la UE y EE. UU. y el creciente número de empresas que se adhieren a los principios de puerto seguro. Después de recordar la estructura y el funcionamiento del puerto seguro, la Comisión insiste en la necesidad de mejorar la aplicación de los principios en las entidades participantes y sus subcontratistas. Según la Comunicación, esto exigiría que los principios de puerto seguro se incorporen de una forma más eficaz a las políticas de protección de la vida privada adoptadas por las entidades participantes y se pongan a disposición del público. La Comisión Federal de Comercio (FTC, por sus siglas en inglés) debería aplicar su cumplimiento con más determinación. Además, las autoridades de protección de datos deberían participar en la concienciación sobre el puerto seguro en la UE y, en particular, sobre la existencia de un grupo de expertos de la UE en protección de datos. La Comisión también aporta soluciones para mejorar los mecanismos de resolución alternativa de litigios.

9. En lo que atañe al acceso a los datos transferidos en el marco de puerto seguro y tratados posteriormente por las autoridades estadounidenses, la Comisión insiste en que no deben utilizarse más allá de lo estrictamente necesario o proporcionado. También exige que se controle cuidadosamente el recurso a excepciones en las políticas de protección de la vida privada para satisfacer exigencias de seguridad nacional, interés público o cumplimiento de la ley, de forma que no se socave la protección ofrecida. También anima a las entidades participantes a que sean transparentes sobre dichas excepciones y sus efectos respecto de la confidencialidad de las comunicaciones para concienciar a los ciudadanos.

I.3. *Ámbito de aplicación y objetivo del presente Dictamen*

10. El presente Dictamen se centra en la Comunicación sobre el restablecimiento de la confianza y, dentro de dicho contexto, también en la Comunicación sobre el puerto seguro. Por consiguiente, no realiza observaciones directas sobre las revelaciones relacionadas con los Estados miembros de la UE, ya sea en colaboración con EE. UU. o por iniciativa propia, ni sobre las actividades de vigilancia por parte de terceros países distintos de EE. UU.

11. El Dictamen comienza formulando observaciones relacionadas con el enfoque general de la Comunicación sobre el restablecimiento de la confianza. En la parte II se analiza brevemente la aplicabilidad del correspondiente marco jurídico y sus consecuencias, y se incluyen observaciones relacionadas con la Comunicación sobre el puerto seguro. Dado que el Grupo de trabajo del artículo 29 ([1]) está examinando en la actualidad los marcos jurídicos de la UE e internacional aplicables, el presente Dictamen no entra en detalle en dicha parte. En la parte III se tratan las recomendaciones de la Comisión sobre los siguientes pasos que deberán adoptarse.

I.4. *Observaciones relativas al enfoque de la Comunicación sobre el restablecimiento de la confianza*

12. La Comunicación se centra en el hecho de que la confianza entre la UE y EE. UU. como socios estratégicos se ha visto afectada de forma negativa por las revelaciones sobre los programas y es necesario restablecer dicha confianza. El SEPD recibe con agrado este reconocimiento.

([1]) El Grupo del artículo 29 para la protección de datos, establecido por la Directiva 95/46/CE, tiene un carácter consultivo y actúa con independencia. Está compuesto por las autoridades nacionales de protección de datos de la UE, el SEPD y la Comisión.

13. Sin embargo, los programas, cuya existencia en algunos casos confirma de forma clara el informe ([1]), no solo afectan a la confianza, sino también a los derechos jurídicos, tal como han quedado establecidos en el Derecho primario y derivado de la UE y del Consejo de Europa, en particular a los derechos de privacidad y protección de los datos. También demuestran la recogida de inteligencia exterior a gran escala que se está produciendo en estos momentos en virtud del marco jurídico de EE. UU. ([2]), tal como ha sido interpretado por el Tribunal Supremo de dicho país ([3]). El informe también confirma la falta de garantías, protecciones, derechos, supervisión y posibilidades de recurso disponibles para los ciudadanos de la UE con arreglo al marco estadounidense ([4]).

14. Tal como la Comisión ha subrayado en repetidas ocasiones, la confianza de los ciudadanos y de las empresas en las comunicaciones de internet depende de que dispongan de herramientas eficaces de protección técnica de la privacidad y, de forma más específica, de la confidencialidad de las comunicaciones. Esta necesidad también ha sido reconocida por el Grupo estadounidense de Revisión sobre Inteligencia y Tecnología de las Comunicaciones ([5]), el cual ha formulado diversas recomendaciones para restablecer la confianza en las herramientas de encriptación y en los programas informáticos comerciales, así como en el funcionamiento de los mecanismos rápidos para solucionar las vulnerabilidades de los programas. La debilidad de la confianza en dichos sistemas ha sido considerada como uno de los efectos más dañinos en los recientes debates sobre las operaciones de inteligencia de señales, por parte de algunos de los expertos en seguridad más reconocidos ([6]). A la vista de la importancia de contar con una ciberseguridad efectiva para Europa, debe desarrollarse a escala europea una respuesta a este desafío técnico y político, basándose en una iniciativa de la Comisión.

15. En el apartado 3 de la Comunicación, la Comisión aborda los pasos futuros que serán necesarios adoptar para restablecer la confianza en las transferencias de datos entre la UE y EE. UU. El SEPD recibe con agrado este apartado, que se centra en la mejora del marco jurídico existente y que propone nuevos instrumentos. Sin embargo, la Comisión no trata el hecho de cómo los instrumentos nacionales, de la UE y del Consejo de Europa se han visto afectados por los programas. El SEPD considera que el impacto sobre los instrumentos jurídicos existentes debería recibir una mayor atención en la Comunicación.

IV. Observaciones finales

79. El SEPD recibe con agrado las medidas consideradas por la Comisión, aunque destaca que las actividades de vigilancia reveladas por las agencias de inteligencia de EE. UU. no solo afectan a la confianza en los flujos de datos entre la UE y EE. UU., sino que también tienen un impacto en los derechos existentes y aplicables de los ciudadanos de la UE al respecto de la privacidad y de la protección de sus datos personales. Estos derechos quedan consagrados tanto en el Derecho primario como en el Derecho derivado de la UE y del Consejo de Europa. Por lo tanto, el SEPD lamenta que la Comunicación sobre el restablecimiento de la confianza no haya concedido una mayor atención al impacto en los instrumentos jurídicos existentes.

80. El SEPD sería partidario de que la Comisión mostrara más ambición en diversos puntos a la hora de definir los pasos siguientes que deben adoptarse y considera que:

— La aplicación y ejecución adecuadas del actual marco jurídico europeo de protección de datos no solo están previstas por la ley sino que también podrían constituir una contribución esencial para restablecer la confianza. Esto también es aplicable a los instrumentos que regulan las transferencias internacionales entre la UE y EE. UU., incluidos los principios de puerto seguro existentes.

— La Comisión debería recordar que las excepciones o limitaciones a los derechos fundamentales que se permiten con fines de seguridad nacional únicamente están justificados y son admisibles si son estrictamente necesarios, proporcionados y conformes con la jurisprudencia del TEDH y del Tribunal de Justicia.

([1]) Véanse las páginas 5, 10 y 26 del informe, en el que, basándose en dictámenes desclasificados del Tribunal de Vigilancia de Inteligencia Exterior, se confirma que «las agencias de inteligencia estadounidenses han recurrido a métodos de recogida con arreglo al artículo 702 con un amplio alcance, como la recogida de datos con el programa PRISM de los proveedores de servicios de Internet o a través de la "recogida hacia arriba" de los datos que son transmitidos en EE. UU.».

([2]) EE. UU. confirmó que existían otras bases jurídicas para la recogida de inteligencia en las que se pueden adquirir los datos de personas no estadounidenses, aunque no ofreció detalles sobre las autoridades ni los procedimientos jurídicos en que resultaban aplicables. No se revelaron todas las bases jurídicas relevantes al Grupo de trabajo (véase la página 13 del informe).

([3]) Véanse las páginas 4 a 12 del informe.

([4]) Véanse las páginas 26 a 27 del informe.

([5]) «Liberty and Security in a Changing World» (Libertad y seguridad en un mundo cambiante), Informe y Recomendaciones del Presidente del Grupo de Revisión sobre Inteligencia y Tecnología de las Comunicaciones, en particular las recomendaciones 25, 29 y 30. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

([6]) B Schneier, C Soghoian en el informe de 6 de septiembre de 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq--encryption-codes-security; B. Preneel: Discurso de clausura del ISSE 2013: «The Cryptographic Year in Review» («Revisión del año criptográfico») http://homes.esat.kuleuven.be/~preneel/preneel_isse13.pdf

— El SEPD está completamente de acuerdo en que la consolidación y la mejora del marco europeo de protección de datos exige una rápida adopción de las propuestas de reforma de la protección de datos con un contenido adecuado, para proporcionar una protección más fuerte, efectiva y coherente de los datos personales y de la privacidad dentro de todo el alcance de la legislación europea. Esto también ofrecería una protección de los datos adecuada en el caso de un uso posterior con fines de aplicación de la ley y ante los posibles conflictos internacionales de jurisdicción.

— Los principios de puerto seguro deben ser revisados y reforzados de conformidad con las líneas indicadas por la Comisión. El SEPD recomienda que se establezcan plazos más estrictos dentro de los cuales deberán adoptarse dichas acciones, incluido un seguimiento adecuado en el caso de que sigan existiendo deficiencias.

— Deben reforzarse las garantías de protección de datos que son aplicables a la cooperación de la UE y EE. UU. en la aplicación de la ley. Las negociaciones en curso sobre un acuerdo marco no deben legitimar las transferencias masivas de datos sino que deberían cumplir con el marco de protección de datos existente y con el resultado de su actual proceso de revisión. En particular, los mecanismos de recurso eficaces deberían ser accesibles a todos los interesados, con independencia de su nacionalidad. Esto también debería ser aplicable en su debido momento a los acuerdos internacionales existentes, cuando resulte necesario basándose en cláusulas transitorias adecuadas.

— La Comisión debería apoyar los esfuerzos de las autoridades y del Congreso de EE. UU. de adoptar una ley general sobre privacidad, que establezca garantías sólidas y una supervisión adecuada, en particular en los ámbitos en que los que actualmente no exista una protección de la privacidad considerable.

— Las negociaciones que están en curso en la actualidad para adoptar una Asociación Transatlántica de Comercio e Inversión (ATCI) no deberían tener un impacto negativo sobre la protección de los datos personales de los ciudadanos. Al mismo tiempo, la Comisión debería considerar el establecimiento de un objetivo común de desarrollo gradual hacia una mayor interoperabilidad de los marcos jurídicos de la protección de datos y la privacidad, al que EE. UU. debería contribuir, tal como se ha mencionado anteriormente.

— La promoción internacional de normas de privacidad debería incluir:

  i) la promoción de la coherencia total de los nuevos instrumentos internacionales con el marco europeo de protección de datos,

  ii) la promoción de la adhesión de terceros países y, en particular, de EE. UU., al Convenio nº 108 del Consejo de Europa,

  iii) el apoyo de la adopción de un instrumento internacional que exija el respecto de las normas de protección de datos por parte de las actividades de inteligencia, lo cual podría adoptarse a escala de la ONU, sobre la base del artículo 17 del PIDCP.

— Debería obligarse a que las actividades de vigilancia observen, en todo momento, el Estado de derecho y los principios de necesidad y proporcionalidad en una sociedad democrática. Por lo tanto, deberían aclararse y, en su caso, complementarse, los marcos jurídicos a todos los niveles relevantes. Estos marcos deberían incluir mecanismos de supervisión adecuados y lo suficientemente sólidos.

— Las instituciones de la UE y todas las entidades relevantes de los Estados miembros son responsables asimismo, en calidad de responsables del tratamiento de los datos, de garantizar una seguridad informática eficaz, lo cual implica llevar a cabo una evaluación del riesgo para la seguridad de los datos a un nivel adecuado. También exige, por un lado, promover la investigación de mecanismos de encriptación y concienciar a los responsables del tratamiento de los datos y a los ciudadanos sobre los riesgos para la privacidad que los productos vendidos o utilizados pueden plantear, y por otro, exigir a los desarrolladores que utilicen métodos de diseño concretos para evitar o, al menos, reducir dichos riesgos. La UE debe liderar iniciativas educativas sobre la seguridad de los datos tratados en Internet.

Hecho en Bruselas, el 20 de febrero de 2014.

Peter HUSTINX

Supervisor Europeo de Protección de Datos