

Programa de vigilancia de la ANS de los EE.UU., servicios de inteligencia en varios Estados miembros e impacto en la privacidad de los ciudadanos de la UE

Resolución del Parlamento Europeo, de 4 de julio de 2013, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en la privacidad de los ciudadanos de la UE (2013/2682(RSP))

El Parlamento Europeo,

- Vistos los artículos 2, 3, 6 y 7 del Tratado de la Unión Europea (TUE) y el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE),
- Vistos la Carta de los Derechos Fundamentales de la Unión Europea y el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales (CEDH),
- Vistos el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, y su Protocolo adicional, de 8 de noviembre de 2001,
- Vista la legislación de la UE sobre el derecho a la privacidad y a la protección de datos, en particular la Directiva 95/46/CE 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, la Decisión marco 2008/977/JAI relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, la Directiva 2002/58/CE relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas, y el Reglamento (CE) n° 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos,
- Vistas las propuestas de la Comisión de un reglamento y una directiva relativos a la reforma del régimen de protección de datos en la UE,
- Vistos el Acuerdo UE-EE.UU. de Asistencia Judicial, que permite el intercambio de datos con fines de prevención e investigación de actividades delictivas, el Convenio sobre la Ciberdelincuencia (CETS n° 185), el Acuerdo de puerto seguro UE-EE.UU. (2000/520/CE) y la revisión en curso del régimen de puerto seguro,
- Vistas la Ley Patriota y la Ley de Vigilancia de Inteligencia Extranjera (FISA) de los Estados Unidos, incluida la Sección 702 de la Ley de modificación de la Vigilancia de Inteligencia Extranjera (FISAA), de 2008,
- Vistas las negociaciones en curso de un acuerdo marco UE-EE.UU. para la protección de los datos personales que se transmiten y procesan para fines de cooperación policial y judicial,
- Vistas sus anteriores resoluciones sobre el derecho a la privacidad y a la protección de

datos, en particular su Resolución, de 5 de septiembre de 2001, sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y comerciales (sistema de interceptación Echelon)¹;

- Vistas las declaraciones del Presidente del Consejo Europeo, Herman van Rompuy, del Presidente del Parlamento Europeo, Martin Schulz, de la Vicepresidenta de la Comisión / Comisaria de Justicia, Derechos Fundamentales y Ciudadanía, Viviane Reding, y del Vicepresidente de la Comisión / Alta Representante de la UE para Asuntos Exteriores y Política de Seguridad, Catherine Ashton,
 - Visto el artículo 110, apartados 2 y 4, de su Reglamento,
- A. Considerando que la asociación transatlántica entre la UE y los EE.UU. se ha de basar en la confianza y el respeto mutuos, la cooperación leal y mutua y el respeto de los derechos fundamentales y el Estado de Derecho;
 - B. Considerando que los Estados miembros están obligados a respetar los derechos y valores fundamentales consagrados en el artículo 2 del TUE y en la Carta de los Derechos Fundamentales;
 - C. Considerando que actualmente se pone en duda la adhesión a dichos principios después de que las noticias aparecidas en la prensa internacional en junio de 2013 hayan revelado pruebas de que, mediante programas como PRISM, las autoridades de los EE.UU. están accediendo a datos personales de ciudadanos de la UE a través de proveedores de servicios en línea estadounidenses, y los están procesando a gran escala;
 - D. Considerando que estas dudas no solo se refieren a acciones de las autoridades estadounidenses, sino también de varios Estados miembros de la UE, que, según la prensa internacional, han cooperado con PRISM y otros programas del mismo tipo o han obtenido acceso a las bases de datos creadas;
 - E. Considerando además que varios Estados miembros disponen de programas de vigilancia de características similares al programa PRISM o están debatiendo la posibilidad de establecer este tipo de programas;
 - F. Considerando que se han planteado cuestiones específicas en relación con la compatibilidad con la legislación de la UE de las prácticas de la agencia de inteligencia del Reino Unido, el Centro Gubernamental de Comunicaciones (GCHQ), que ha intervenido directamente cables submarinos transatlánticos que transmitían comunicaciones electrónicas, en el marco de un programa cuyo nombre en clave es Tempora; que hay noticias de que otros Estados miembros acceden a comunicaciones electrónicas transnacionales sin una orden regular, pero sobre la base de tribunales especiales, comparten datos con otros países (Suecia), y pueden aumentar sus capacidades de vigilancia (Países Bajos, Alemania); y que en otros Estados miembros se ha expresado preocupación en cuanto a los poderes de interceptación de los servicios secretos (Polonia);
 - G. Considerando que existen indicios de que instituciones de la UE y embajadas y representaciones de la UE y de los Estados miembros han estado sometidas a la vigilancia y a actividades de espionaje de los EE.UU.;

¹ DO C 72 E de 21.3.2002, p. 221.

- H. Considerando que la Comisaria Reding ha enviado una carta al Fiscal General de los EE.UU., Eric Holder, en la que expone las preocupaciones europeas y pide aclaraciones y explicaciones sobre el programa PRISM y otros programas análogos de recopilación y búsqueda de datos, y sobre las leyes en virtud de las cuales pueden autorizarse tales programas; y que aún no se ha recibido una respuesta completa de las autoridades de los EE.UU., a pesar de los debates mantenidos en la reunión de Ministros de Justicia UE-EE.UU. celebrada en Dublín el 14 de junio de 2013;
- I. Considerando que, en virtud del Acuerdo de puerto seguro, se confía a los Estados miembros y a la Comisión el cometido de garantizar la seguridad y la integridad de los datos personales; que, según la prensa internacional, todas las empresas implicadas en el caso PRISM son Partes en el Acuerdo de puerto seguro; y que, de conformidad con el artículo 3 del mismo, de no ser respetadas las disposiciones del Acuerdo, la Comisión tiene el deber de revocarlo o suspenderlo;
- J. Considerando que en el Acuerdo UE-EE.UU. de Asistencia Judicial, ratificado por la Unión y por el Congreso de los EE.UU., se estipulan modalidades de recopilación e intercambio de información, así como para solicitar y prestar asistencia para obtener pruebas localizadas en un país a fin de prestar asistencia para investigaciones o procedimientos penales en otro país;
- K. Considerando que sería desafortunado que los esfuerzos para concluir una Asociación Transatlántica de Comercio e Inversión (ATCI), que demuestra el compromiso de reforzar más la cooperación entre la UE y los EE.UU., se vieran afectados por las acusaciones vertidas recientemente;
- L. Considerando que el 14 de junio de 2013 la Comisaria Malmström anunció la creación de un grupo transatlántico de expertos;
- M. Considerando que la Comisaria Reding ha escrito a las autoridades del Reino Unido para expresar su preocupación ante las noticias aparecidas en los medios de comunicación sobre el programa Tempora y pedir aclaraciones sobre su ámbito de aplicación y funcionamiento; y que las autoridades británicas han defendido las actividades de vigilancia del GCHQ y han afirmado que operan con arreglo a unas directrices estrictas y legales;
- N. Considerando que la reforma de la protección de datos está en curso a nivel de la UE mediante la revisión de la Directiva 95/46/CE y su sustitución por los propuestos Reglamento general sobre protección de datos y Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos;
1. Expresa, al tiempo que confirma su apoyo continuado a los esfuerzos transatlánticos en la lucha contra el terrorismo y la delincuencia organizada, su seria preocupación ante PRISM y otros programas similares, pues, de confirmarse la información disponible por ahora, representarían una grave violación del derecho fundamental a la privacidad y la protección de los datos de los ciudadanos y los residentes de la UE, así como del derecho a la vida privada y familiar, la confidencialidad de las comunicaciones, la presunción de inocencia, la libertad de expresión, la libertad de información y la libertad de empresa;

2. Condena enérgicamente el espionaje de las representaciones de la UE, pues, de confirmarse la información disponible por ahora, supondría una grave violación de la Convención de Viena sobre Relaciones Consulares, aparte de su posible repercusión en las relaciones transatlánticas; pide que las autoridades estadounidenses aclaren inmediatamente esta cuestión;
3. Pide a las autoridades de los EE.UU. que faciliten sin demoras injustificadas a la UE información completa sobre el programa PRISM y otros programas similares que sirvan para la recogida de datos, particularmente en lo que respecta a su base legal, necesidad y proporcionalidad, así como a las salvaguardas aplicadas para proteger los derechos fundamentales de los ciudadanos de la UE, como la limitación del alcance y la duración, las condiciones de acceso y la supervisión independiente, como se prevé en el Convenio sobre la Ciberdelincuencia y solicitó la Comisaria Reding en su carta de 10 de junio de 2013 al Fiscal General Eric Holder; pide a las autoridades de los EE.UU. que suspendan y revisen todas aquellas leyes y programas de vigilancia que violen el derecho fundamental de los ciudadanos de la UE a la privacidad y a la protección de sus datos, la soberanía y jurisdicción de la UE y sus Estados miembros, y el Convenio sobre Ciberdelincuencia;
4. Pide a la Comisión, al Consejo y a los Estados miembros que tomen en consideración todos los instrumentos de que disponen en los debates y negociaciones con los EE.UU., tanto a escala política como de expertos, a fin de alcanzar los objetivos mencionados, incluida la posible suspensión de los acuerdos sobre el registro de nombres de los pasajeros (PNR) y sobre el Programa de Seguimiento de la Financiación del Terrorismo (TFTP);
5. Pide que se otorgue al grupo de expertos transatlántico, anunciado por la Comisaria Malmström y el que participará el Parlamento, un nivel adecuado de habilitación de seguridad y acceso a todos los documentos pertinentes, de manera que pueda realizar su trabajo correctamente y en un plazo preestablecido; pide asimismo que el Parlamento cuente con una representación adecuada en este grupo de expertos;
6. Pide a la Comisión y a las autoridades de los EE.UU. que reanuden sin demora las negociaciones sobre el acuerdo marco para la protección de los datos personales que se transmiten y procesan para fines de cooperación policial y judicial; pide a la Comisión que, durante dichas negociaciones, vele por que el acuerdo cumpla al menos los siguientes criterios:
 - a) que se otorgue a los ciudadanos de la UE el derecho a la información cuando sus datos se procesen en los EE.UU.;
 - b) que se garantice que el acceso de los ciudadanos de la UE al sistema judicial de los EE.UU. sea idéntico al que disfrutaban los ciudadanos estadounidenses;
 - c) que se conceda el derecho de recurso en particular;
7. Pide a la Comisión que vele por que no se menoscaben las normas de la UE en materia de protección de datos, ni las negociaciones en curso sobre el paquete sobre protección de datos de la UE, como resultado de la Asociación Transatlántica de Comercio e Inversión (ATCI) con los EE.UU.;
8. Pide a la Comisión que lleve a cabo una revisión completa del Acuerdo de puerto seguro a la luz de las recientes revelaciones, en virtud del artículo 3 de dicho Acuerdo;

9. Expresa su profunda preocupación ante las revelaciones de supuestos programas de vigilancia aplicados por Estados miembros, con la ayuda de la Agencia Nacional de Seguridad de los EE.UU. (NSA) o unilateralmente; pide a los Estados miembros que examinen la compatibilidad de estos programas con el Derecho primario y secundario de la UE, en particular el artículo 16 del TFUE relativo a la protección de datos, y con las obligaciones en materia de derechos fundamentales de la UE que se derivan del CEDH y de las tradiciones constitucionales comunes de los Estados miembros;
10. Destaca que todas las empresas que ofrezcan servicios en la UE deben cumplir el Derecho de la UE sin excepción y son responsables de las infracciones que cometan;
11. Destaca que las empresas que operen bajo la jurisdicción de terceros países deben advertir de manera clara e inequívoca a los usuarios ubicados en la UE de la posibilidad de que sus datos personales sean procesados por agencias policiales y de inteligencia a raíz de órdenes o requerimientos secretos;
12. Lamenta que la Comisión haya suprimido el antiguo artículo 42 de la versión del Reglamento relativo a la protección de datos que se ha filtrado; pide a la Comisión que aclare las razones por las que actuó de ese modo; pide al Consejo que siga el planteamiento del Parlamento y vuelva a incluir dicha disposición;
13. Subraya que, en los Estados democráticos y abiertos basados en el Estado de Derecho, los ciudadanos tienen derecho a conocer las violaciones graves de sus derechos fundamentales y a denunciarlas, incluidas aquellas en que estén implicados sus propios Gobiernos; destaca la necesidad de unos procedimientos que permitan a los denunciantes desvelar violaciones graves de los derechos fundamentales y de que se brinde a estas personas la protección necesaria, también a escala internacional; expresa su apoyo constante al periodismo de investigación y a la libertad de los medios de comunicación;
14. Pide al Consejo, con carácter de urgencia, que agilice su trabajo sobre el conjunto del paquete sobre protección de datos y, más específicamente, sobre la Directiva relativa a la protección de datos propuesta;
15. Subraya la necesidad de establecer un órgano europeo equivalente a las comisiones de control e investigación parlamentarias-judiciales mixtas sobre los servicios de inteligencia que existen actualmente en algunos Estados miembros;
16. Encarga a su Comisión de Libertades Civiles, Justicia y Asuntos de Interior que realice una investigación exhaustiva sobre este asunto en colaboración con los Parlamentos nacionales y el grupo de expertos UE-EE.UU. creado por la Comisión, y que informe al respecto antes de finales de año, para lo cual:
 - a) recopilará toda la información y las pruebas pertinentes a partir de fuentes tanto estadounidenses como de la UE (investigación);
 - b) investigará las supuestas actividades de vigilancia de las autoridades estadounidenses y también las que hayan podido realizar determinados Estados miembros (localización de responsabilidades);
 - c) evaluará el impacto de los programas de vigilancia en lo que respecta a los siguientes aspectos: los derechos fundamentales de los ciudadanos de la UE (particularmente el

derecho al respeto de la vida privada y a las comunicaciones privadas, la libertad de expresión, la presunción de inocencia y el derecho a un recurso efectivo); la protección real de los datos tanto dentro de la UE como para los ciudadanos de la UE residentes fuera de la UE, centrándose particularmente en la efectividad de la legislación de la UE respecto de los mecanismos de extraterritorialidad; la seguridad de la UE en la era de la computación en nube; el valor añadido y la proporcionalidad de estos programas en lo que respecta a la lucha contra el terrorismo; la dimensión exterior del espacio de libertad, seguridad y justicia (evaluando la validez de las decisiones de idoneidad para las transferencias de la UE a terceros países, como las que se realizan en el marco del Acuerdo de puerto seguro, acuerdos internacionales y otros instrumentos jurídicos que prevén cooperación y asistencia jurídicas) (análisis de los daños y del riesgo);

- d) explorará los mecanismos más apropiados de recurso en caso de incumplimientos confirmados (recurso administrativo y judicial y regímenes de compensación);
 - e) presentará recomendaciones para impedir nuevos incumplimientos y garantizar una protección de alto nivel y creíble de los datos personales de los ciudadanos de la UE a través de los medios adecuados, en particular la adopción de un paquete integral de protección de datos (recomendaciones sobre políticas y elaboración de legislación);
 - f) emitirá recomendaciones para reforzar la seguridad de las TI en las instituciones, los órganos y las agencias de la UE, mediante normas internas adecuadas en materia de seguridad para los sistemas de comunicación, con el fin de prevenir y poner remedio al acceso no autorizado y a la divulgación o la pérdida de información y datos personales (resolución de las violaciones de la seguridad);
17. Encarga a su Presidente que transmita la presente Resolución a la Comisión, al Consejo, al Consejo de Europa, a los Parlamentos de los Estados miembros, al Presidente de los EE.UU., al Senado y a la Cámara de Representantes de los EE.UU., así como a los Secretarios de Estado de Seguridad del Territorio Nacional y de Justicia de los EE.UU.