Comisión de Libertades Civiles, Justicia y Asuntos de Interior

2013/2188(INI)

8.1.2014

PROYECTO DE INFORME

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 los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior

(2013/2188(INI))

Comisión de Libertades Civiles, Justicia y Asuntos de Interior

Ponente: Claude Moraes

ÍNDICE

ÍNDICE

Página

PROPUESTA DE RESOLUCIÓN DEL PARLAMENTO EUROPEO

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 los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior
(2013/2188(INI))

El Parlamento Europeo,

– Visto el Tratado de la Unión Europea (TUE) y, en particular, sus artículos 2, 3, 4, 5, 6, 7, 10, 11 y 21,

– Visto el Tratado de Funcionamiento de la Unión Europea (TFUE) y, en particular sus artículos 15, 16 y 218 y su título V,

– Visto el Protocolo nº 36 sobre las disposiciones transitorias y su artículo 10, así como la Declaración nº 50 relativa a dicho protocolo,

– Vista la Carta de los Derechos Fundamentales de la Unión Europea y, en particular, sus artículos 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 y 52,

– Visto el Convenio Europeo de Derechos Humanos y, en particular, sus artículos 6, 8, 9, 10 y 13 y sus protocolos,

– Vista la Declaración Universal de Derechos Humanos y, en particular, sus artículos 7, 8, 10,11,12 y 14[1],

– Visto el Pacto Internacional de Derechos Civiles y Políticos y, en particular, sus artículos 14, 17, 18 y 19,

– visto el Convenio del Consejo de Europa sobre protección de datos (ETS nº 108) y su Protocolo Adicional, de 8 de noviembre de 2001, al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, relativo a las autoridades de control y los flujos de datos transfronterizos (ETS nº 181),

– Visto el Convenio del Consejo de Europa sobre la Ciberdelincuencia (ETS nº 185),

– Visto el informe del Relator Especial de las Naciones Unidas sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, presentado el 17 de mayo de 2010[2],

– Visto el informe del Relator Especial de las Naciones Unidas sobre la promoción y la protección de la libertad de opinión y expresión, presentado el 17 de abril de 2013[3],

[1] http://www.un.org/en/documents/udhr/
[2] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement
[3] http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

– Vistas las Directrices sobre los derechos humanos y la lucha contra el terrorismo adoptadas por el Comité de Ministros del Consejo de Europa el 11 de julio de 2002,

– Vista la Declaración de Bruselas, de 1 de octubre de 2010, adoptada por la Sexta Conferencia de las Comisiones Parlamentarias encargadas de la Supervisión de los Servicios de Inteligencia y Seguridad de los Estados miembros de la Unión Europea,

– Vista la Resolución de la Asamblea Parlamentaria del Consejo de Europa nº 1954 (2013) sobre seguridad nacional y acceso a la información,

– Visto el informe sobre la supervisión democrática de los servicios de seguridad adoptado por la Comisión de Venecia el 11 de junio de 2007[1], y en espera con gran interés de su actualización, prevista para la primavera de 2014,

– Vistos los testimonios de los representantes de las comisiones de supervisión de los órganos de inteligencia de Bélgica, Países Bajos, Dinamarca y Noruega,

– Vistos los asuntos presentados ante los tribunales franceses[2], polacos y británicos[3], y ante el Tribunal Europeo de Derechos Humanos[4], en relación con los sistemas de vigilancia masiva,

– Visto el Convenio establecido por el Consejo de conformidad con el artículo 34 del Tratado de la Unión Europea relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea y, en particular, su título III[5],

– Vista la Decisión nº 520/2000 de la Comisión, de 26 de julio de 2000, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América,

– Vistos los informes de evaluación de la Comisión sobre la aplicación de los principios de puerto seguro de 13 de febrero de 2002 (SEC(2002)196) y 20 de octubre de 2004 (SEC(2004)1323),

– Vistas la Comunicación de la Comisión, de 27 de noviembre de 2013, sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE (COM(2013)0847) y la Comunicación de la Comisión, de 27 de noviembre, titulada «Restablecer la confianza en los flujos de datos entre la UE y los EE.UU.» (COM(2013)0846),

– Vistas su Resolución, de 5 de julio de 2000, sobre el proyecto de decisión de la Comisión relativa a la adecuación de la protección garantizada por los principios

[1] http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx
[2] La Fédération Internationale des Ligues des Droits de l'Homme y La Ligue française pour la défense des droits de l'Homme et du Citoyen contra X; Tribunal de Grande Instance of Paris.
[3] Casos de Privacy International y Liberty en el Tribunal de Poderes Investigadores.
[4] Solicitud conjunta en virtud del artículo 34 de Big Brother Watch, Open Rights Group, English Pen Dr Constanze Kurz (demandantes) contra el Reino Unido (demandado).
[5] DO C 197 de 12.7.2000, p. 1.

estadounidenses de puerto seguro y preguntas más frecuentes relacionadas publicadas por el Departamento de Comercio de los EE.UU., que consideraba que no podía confirmarse la adecuación del sistema[1], y los dictámenes del Grupo de Trabajo del Artículo 29, más concretamente el dictamen 4/2000, de 16 de mayo de 2000[2],

– Vistos los acuerdos entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros (acuerdo PNR) de 2004, 2007[3] y 2012[4],

– Vista la revisión conjunta de la aplicación del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos[5], que acompaña al Informe de la Comisión al Parlamento Europeo y al Consejo sobre la revisión conjunta (COM(2013)0844),

– Visto el dictamen del Abogado General Cruz Villalón, en el que se concluye que la Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones es en su conjunto incompatible con el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y que su artículo 6 es incompatible con los artículos 7 y 52, apartado 1, de la Carta[6],

– Vistas la Decisión nº 2010/412/UE del Consejo, de 13 de julio de 2010, relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo (TFTP)[7] y las declaraciones de las Comisión y del Consejo que la acompañan,

– Visto el Acuerdo de Asistencia Judicial entre la Unión Europea y los Estados Unidos de América[8],

– Vistas las negociaciones en curso sobre un acuerdo marco UE-EE.UU. sobre la protección de datos personales transferidos y tratados a efectos de prevención, investigación, descubrimiento y represión de las infracciones penales, incluido el terrorismo, en el marco de la cooperación policial y judicial en materia penal («acuerdo marco»),

– Visto el Reglamento (CE) nº 2271/96 del Consejo, de 22 de noviembre de 1996, relativo a la protección contra los efectos de la aplicación extraterritorial de la legislación adoptada por un tercer país, y contra las acciones basadas en ella o

[1] DO C 121 de 24.4.2001, p. 152.
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32es.pdf
[3] DO L 204 de 4.8.2007, p. 18.
[4] DO L 215 de 11.08.12, p. 5.
[5] SEC(2013)0630 de 27.11.2013.
[6] Dictamen del Abogado General Cruz Villalón, de 12 de diciembre 2013, en el asunto C-293/12.
[7] DO L 195 de 27.7.2010, p. 3.
[8] DO L 181 de 19.7.2003, p. 34.

derivadas de ella[1],

– Vistos la declaración de la Presidenta de la República Federativa de Brasil en la inauguración de la 68ª sesión de la Asamblea General de las Naciones Unidas de 24 de septiembre de 2013 y el trabajo realizado por la Comisión Parlamentaria de investigación sobre el espionaje establecida por el Senado Federal de Brasil,

– Vista la Ley Patriótica («Patriot Act») de los Estados Unidos, firmada por el Presidente George W. Bush el 26 de octubre de 2001,

– Vistas la Ley de vigilancia de inteligencia exterior (FISA) de 1978 y la Ley modificativa de la FISA de 2008,

– Visto el Decreto nº 12333, emitido por el Presidente de los Estados Unidos en 1981 y modificado en 2008,

– Vistas las propuestas legislativas que están siendo examinadas actualmente en el Congreso de los EE.UU., en particular el proyecto de Ley sobre libertades de los EE.UU.,

– Vistas las revisiones realizadas por la Junta de Supervisión de la intimidad y las libertades civiles, el Consejo de Seguridad Nacional de Estados Unidos y el Grupo de Revisión del Presidente sobre Inteligencia y Tecnología de la Comunicaciones, en especial el informe de este último, de 12 de diciembre de 2013, titulado «Liberty and Security in a Changing World» (Libertad y seguridad en un mundo cambiante),

– Vista la sentencia del tribunal de distrito de Estados Unidos del Distrito de Columbia en el asunto Klayman et al. contra Obama et al., acción civil nº 13-0851 de 16 de diciembre de 2013,

– Visto el informe relativo a las conclusiones de los copresidentes de la UE del grupo de trabajo ad hoc UE-EE.UU. sobre protección de datos de 27 de noviembre de 2013[2],

– Vistas sus Resoluciones, de 5 de septiembre de 2001 y 7 de noviembre de 2002, sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y comerciales (sistema de interceptación Echelon),

– Vista su Resolución, de 21 de mayo de 2013, sobre la Carta de la UE: normas para la libertad de los medios de comunicación en la UE[3],

– Vista su Resolución, de 4 de julio de 2013, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los Estados Unidos, los órganos de vigilancia en diversos Estados miembros y su impacto en la privacidad de los ciudadanos de la UE, por la cual encargó a su Comisión de Libertades Civiles, Justicia y Asuntos de Interior

[1] DO L 309 de 29.11.1996, p.1.
[2] Documento 16987/13 del Consejo.
[3] Textos Aprobados, P7_TA(2013)0203.

que llevara a cabo una investigación en profundidad de la cuestión[1],

– Vista su Resolución, de 23 de octubre de 2013, sobre la delincuencia organizada, la corrupción y el blanqueo de dinero: recomendaciones sobre las acciones o iniciativas que han de llevarse a cabo[2],

– Vista su Resolución, de 23 de octubre de 2013, sobre la suspensión del acuerdo TFTP a raíz de la vigilancia de la NSA[3],

– Vista su Resolución, de 10 de diciembre de 2013, sobre la liberación del potencial de la computación en la nube en Europa[4],

– Visto el Acuerdo interinstitucional entre el Parlamento Europeo y el Consejo sobre la transmisión al Parlamento Europeo y la gestión por el mismo de la información clasificada en posesión del Consejo sobre asuntos distintos de los pertenecientes al ámbito de la política exterior y de seguridad común[5],

– Visto el anexo VIII de su Reglamento,

– Visto el artículo 48 de su Reglamento,

– Visto el informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (A7-0000/2013),

El impacto de la vigilancia masiva

A. Considerando que los lazos entre Europa y los Estados Unidos de América se basan en el espíritu y los principios de democracia, libertad, justicia y solidaridad;

B. Considerando que la confianza y el entendimiento mutuos son factores claves en el diálogo transatlántico;

C. Considerando que, en septiembre de 2001, el mundo entró en una nueva fase en la que la lucha contra el terrorismo pasó a formar parte de las principales prioridades de la mayoría de los gobiernos; considerando que las revelaciones basadas en los documentos filtrados de Edward Snowden, excontratista de la Agencia Nacional de Seguridad, obligaron a los líderes elegidos democráticamente a abordar los retos del aumento de las capacidades de las agencias de inteligencia en las actividades de vigilancia y sus repercusiones para el Estado de Derecho en una sociedad democrática;

D. Considerando que las revelaciones que se han producido desde junio de 2013 han suscitado gran inquietud dentro de la UE en lo referente:

- al alcance de los sistemas de vigilancia descubiertos tanto en los Estados

[1] Textos Aprobados, P7_TA(2013)0322.
[2] Textos Aprobados P7_TA(2013)0444.
[3] Textos Aprobados P7_TA(2013)0449.
[4] Textos Aprobados P7_TA(2013)0535.
[5] DO C 353 E de 3.12.2013, pp. 156-167.

Unidos como en los Estados miembros de la UE;

- al alto riesgo de violación de las normas jurídicas y en materia de derechos fundamentales y protección de datos de la UE;
- al grado de confianza entre los socios trasatlánticos de la UE y los EE.UU.;
- al grado de cooperación y participación de determinados Estados miembros de la UE en los programas de vigilancia estadounidenses o programas equivalentes a nivel nacional, como han revelado los medios de comunicación;
- al grado de control y supervisión eficaz de las autoridades políticas de los Estados Unidos y de determinados Estados miembros de la UE sobre sus comunidades de inteligencia;
- a la posibilidad de que estas operaciones de vigilancia masiva se utilicen por motivos distintos a la seguridad nacional y a la estricta lucha contra el terrorismo, por ejemplo, para el espionaje económico e industrial o la elaboración de perfiles por razones políticas;
- a las respectivas funciones y al grado de implicación de las agencias de inteligencia y empresas privadas de informática y telecomunicaciones;
- a las fronteras cada vez más difusas entre el cumplimiento de las leyes y las actividades de inteligencia, lo cual conlleva que todos los ciudadanos sean tratados como sospechosos;
- a las amenazas a la intimidad en una era digital;

E. Considerando que la magnitud sin precedentes del espionaje manifestado requiere una investigación completa por parte de las autoridades de los Estados Unidos, las instituciones europeas y los Gobiernos y Parlamentos nacionales de los Estados miembros;

F. Considerando que las autoridades estadounidenses han negado parte de la información revelada pero no han rebatido la mayor parte de esta; que el debate público se ha desarrollado a gran escala en los Estados Unidos y en un número limitado de Estados miembros de la UE; y que los Gobiernos de la UE guardan silencio con demasiada frecuencia y no ponen en marcha investigaciones adecuadas;

G. Considerando que las instituciones europeas tienen el deber de garantizar que el Derecho de la UE se aplique plenamente en beneficio de los ciudadanos europeos y que la fuerza jurídica de los tratados de la UE no sea menoscabada por la aceptación displicente de los efectos extraterritoriales de las normas o acciones de terceros países;

Avances en los Estados Unidos por lo que se refiere a la reforma de la inteligencia

H. Considerando que el tribunal de distrito del Distrito de Columbia, en su decisión de 16 de diciembre de 2013, ha resuelto que la recopilación de metadatos en bloque por parte de la Agencia Nacional de Seguridad infringe la cuarta enmienda de la

Constitución estadounidense[1];

I. Considerando que una decisión del tribunal de distrito del Distrito Oriental de Michigan ha resuelto que la cuarta enmienda requiere justificación en todas las investigaciones, garantías previas para toda investigación razonable, garantías basadas en causas probables existentes anteriormente, así como especificidad en lo referente a las personas, lugares y objetos y la interposición de un magistrado neutral entre los agentes encargados de garantizar la ley y los ciudadanos[2];

J. Considerando que, en su informe de 12 de diciembre de 2013, el Grupo de Revisión del Presidente sobre Inteligencia y Tecnología de la Comunicaciones propone 45 recomendaciones al Presidente de Estados Unidos; considerando que las recomendaciones destacan la necesidad de proteger simultáneamente la seguridad nacional, la intimidad personal y las libertades civiles; considerando que, a este respecto, invita al Gobierno estadounidense a que ponga fin a la recopilación en bloque de registros telefónicos de personas estadounidenses en virtud de la sección 215 de la Ley Patriótica tan pronto como sea posible, a que lleve a cabo una profunda revisión de la Agencia Nacional de Seguridad y del marco jurídico de la inteligencia de los Estados Unidos con el fin de garantizar el respeto del derecho a la intimidad, a que ponga fin a los esfuerzos para alterar o fabricar software comercial vulnerable (puertas traseras y software malicioso), a que aumente el uso del cifrado, especialmente en el caso de datos en tránsito, y a que no menoscabe los esfuerzos para crear normas de cifrado, a que cree un abogado de interés público que defienda la intimidad y las libertades civiles ante el Tribunal de Vigilancia de Inteligencia Exterior, a que confiera a la Junta de Supervisión de la intimidad y las libertades civiles el poder de supervisar las actividades de la Comunidad de Inteligencia para fines de inteligencia, y no solo para fines contra el terrorismo, a que reciba reclamaciones de los denunciantes, haga uso de los Tratados de Asistencia Judicial Mutua y no utilice la vigilancia para sustraer secretos industriales o comerciales;

K. Considerando que, con respecto a las actividades de inteligencia sobre ciudadanos no estadounidenses en virtud de la sección 702 de la FISA, las recomendaciones al Presidente de los Estados Unidos reconocen la cuestión fundamental del respeto de la intimidad y la dignidad humana consagrado en el artículo 17 de la Declaración Universal de los Derechos Humanos y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos; y que no recomiendan la concesión de los mismos derechos y protecciones a los ciudadanos no estadounidenses que a los estadounidenses;

Marco jurídico

Derechos fundamentales

L. Considerando que el informe sobre las conclusiones de los copresidentes de la UE del Grupo de Trabajo UE-EE.UU. sobre protección de datos proporciona una visión general de la situación jurídica en Estados Unidos, pero no ha ayudado lo suficiente a

[1] Klayman et al. contra Obama et al., acción civil nº 13-0851, 16 de diciembre de 2013.
[2] ACLU contra Agencia Nacional de Seguridad, nº 06-CV-10204, 17 de agosto de 2006.

establecer los hechos relativos a los programas de vigilancia estadounidenses; y que no hay información disponible sobre el denominado Grupo de Trabajo «segunda vía», conforme al cual los Estados miembros debaten bilateralmente con las autoridades estadounidenses las cuestiones relativas a la seguridad nacional;

M. Considerando que los derechos fundamentales, en particular la libertad de expresión, de prensa, de pensamiento, de conciencia, de religión y de asociación, la vida privada, la protección de datos, así como el derecho a un recurso efectivo, la presunción de inocencia y el derecho a un juicio justo y a no ser discriminado, consagrados en la Carta de los Derechos Fundamentales de la Unión Europea y en la Convención Europea de los Derechos Humanos, son las piedras angulares de la democracia;

Competencias de la Unión Europea en materia de seguridad

N. Considerando que, de conformidad con el artículo 67, apartado 3 del TFUE, la UE se esforzará por garantizar un elevado nivel de seguridad; que las disposiciones del Tratado (en particular, el artículo 4, apartado 2, del TUE, el artículo 72 del TFUE y el artículo 73 del TFUE) implican que la UE dispone de determinadas competencias en asuntos relativos a la seguridad colectiva de la Unión; y que la UE ha ejercido su competencia en asuntos de seguridad interna decidiendo sobre varios instrumentos legislativos y celebrando acuerdos internacionales (PNR, TFTP) orientados a luchar contra el terrorismo y los delitos graves y creando una estrategia de seguridad interna y agencias que trabajan en este ámbito;

O. Considerando que los conceptos de «seguridad nacional», «seguridad interna», «seguridad interna de la UE» y «seguridad internacional» se superponen; y que la Convención de Viena sobre el Derecho de los Tratados, el principio de cooperación leal entre los Estados miembros de la UE y el principio del Derecho en materia de derechos humanos de interpretar cualquier excepción en un sentido estricto apuntan a una interpretación restrictiva del concepto de «seguridad nacional» y obligan a los Estados miembros a abstenerse de invadir las competencias de la UE;

P. Considerando que, en virtud del CEDH, las agencias de los Estados miembros e incluso las partes privadas que actúan en el campo de la seguridad nacional también tienen que respetar los derechos contemplados en aquel, ya sean los de sus propios ciudadanos o de los ciudadanos de otros Estados; y que lo anterior también es aplicable a otras autoridades de los Estados en el ámbito de la seguridad nacional;

Extraterritorialidad

Q. Considerando que la aplicación extraterritorial por parte de un tercer país de sus leyes, legislaciones y otros instrumentos legislativos y ejecutivos en las situaciones recogidas por la jurisdicción de la UE o sus Estados miembros puede repercutir en el ordenamiento jurídico establecido y en el Estado de Derecho, o incluso infringir el Derecho internacional o de la UE, incluidos los derechos de personas físicas y jurídicas, habida cuenta del alcance y el objetivo declarado o real de dicha aplicación; y que, en estas circunstancias excepcionales, es necesario adoptar medidas a nivel europeo para garantizar el respeto del Estado de Derecho y los derechos de las personas físicas y jurídicas dentro de la UE, en concreto, eliminando, neutralizando,

bloqueando o luchando contra los efectos de la legislación extranjera pertinente;

Transferencias internacionales de datos

R. Considerando que la transferencia de datos personales por parte de las instituciones, organismos, oficinas o agencias de la UE o por parte de los Estados miembros a los Estados Unidos con fines policiales en ausencia de garantías y protecciones adecuadas para el respeto de los derechos fundamentales de los ciudadanos de la UE, en particular los derechos a la intimidad y la protección de datos personales, conllevaría que dicha institución, organismo, oficina o agencia de la UE o dicho Estado miembro sean responsables, en virtud del artículo 340 del TFUE o de la jurisprudencia establecida por el Tribunal de Justicia de la Unión Europea[1], de infracción del Derecho de la UE, que incluye cualquier infracción de los derechos fundamentales recogidos en la Carta de la UE;

Transferencias a Estados Unidos sobre la base del acuerdo de puerto seguro

S. Considerando que el marco jurídico de protección de datos de los EE.UU. no garantiza un nivel adecuado de protección para los ciudadanos europeos;

T. Considerando que, para que los responsables del tratamiento de datos de la UE puedan transferir datos personales a una entidad en los EE.UU., la Comisión, en su Decisión 520/2000, ha confirmado la adecuación de la protección conferida por los principios de puerto seguro de respeto de la intimidad y las preguntas más frecuentes relacionadas emitidas por el Departamento de Comercio de Estados Unidos para los datos personales transferidos desde la Unión a organizaciones establecidas en Estados Unidos que cumplan con los principios de puerto seguro;

U. Considerando que, en su Resolución de 5 de julio de 2000, el Parlamento Europeo expresó sus dudas e inquietudes acerca de la adecuación de los principios de puerto seguro y pidió a la Comisión que revisara la decisión con prontitud a la luz de la experiencia y de los desarrollos legislativos;

V. Considerando que la Decisión 520/2000 de la Comisión estipula que las autoridades competentes en los Estados miembros pueden ejercer sus poderes actuales para suspender el flujo de datos a una organización que haya autocertificado su adhesión a los principios de puerto seguro, con el fin de proteger a los individuos en relación con el procesamiento de sus datos personales en los casos en que exista la probabilidad sustancial de que estos principios no se estén respetando o cuando la continuación de la transferencia provoque un riesgo inminente de daños graves para los interesados;

W. Considerando que la Decisión 520/2000 de la Comisión también establece que, cuando se hayan proporcionado pruebas de que un responsable de garantizar el cumplimiento de los principios no está desempeñando su función adecuadamente, la Comisión deberá informar al Departamento de Comercio de los Estados Unidos y, si es necesario, presentar medidas para revertir o suspender dicha Decisión o limitar su

[1] Véanse especialmente los asuntos acumulados C-6/90 y C-9/90, Francovich y otros contra Italia, sentencia de 28 de mayo de 1991.

alcance;

X. Considerando que, en sus dos primeros informes sobre la aplicación de los principios de puerto seguro, de 2002 y 2004, la Comisión identificó varias deficiencias en lo que respecta a la aplicación adecuada de los principios de puerto seguro y realizó diversas recomendaciones a las autoridades estadounidenses con el fin de rectificarlas;

Y. Considerando que, en su tercer informe de aplicación, de 27 de noviembre de 2013, nueve años después del segundo informe y sin que se haya rectificado ninguna de las deficiencias reconocidas en dicho informe, la Comisión identificó deficiencias y defectos adicionales de amplio alcance en el mecanismo de puerto seguro y concluyó que no podía mantenerse la aplicación actual; que la Comisión ha subrayado que el amplio acceso de las agencias de inteligencia estadounidenses a los datos transferidos a los EE.UU. por las entidades con certificación de puerto seguro plantea importantes interrogantes adicionales sobre la continuidad de la protección de los datos de los interesados en la UE; y que la Comisión dirigió 13 recomendaciones a las autoridades estadounidenses y se comprometió a identificar para el verano de 2014, junto con las autoridades estadounidenses, un paquete de medidas correctivas que habían de aplicarse lo antes posible, creando la base para una revisión total del funcionamiento de los principios de puerto seguro;

Z. Considerando que, entre el 28 y el 31 de octubre de 2013, la delegación de la Comisión del Parlamento Europeo sobre Libertades Civiles, Justicia y Asuntos de Interior (Comisión LIBE) que acudió a Washington D.C. se reunió con el Departamento de Comercio y la Comisión Federal de Comercio de Estados Unidos; que el Departamento de Comercio reconoció la existencia de organizaciones que han autocertificado su adhesión a los principios de puerto seguro pero que claramente muestran una «condición no actual», lo que significa que la empresa no cumple con los requisitos de puerto seguro aunque continúe recibiendo datos personales de la UE; y que la Comisión Federal de Comercio admitió que deberían revisarse los principios de puerto seguro para mejorarlos, particularmente en relación con las reclamaciones y los sistemas de resolución de litigios alternativos;

AA. Considerando que los principios de puerto seguro pueden limitarse «en la medida en que resulte necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley»; que, como excepción a un derecho fundamental, dicha excepción siempre debe interpretarse restrictivamente y limitarse a lo que se considera necesario y proporcionado en una sociedad democrática, y la ley debe establecer claramente las condiciones y garantías para que dicha limitación sea legítima; y que dicha excepción no debe utilizarse de forma que menoscabe la protección garantizada por la ley de protección de datos de la UE y los principios de puerto seguro;

AB. Considerando que el acceso a gran escala de las agencias de inteligencia de los EE.UU. ha minado gravemente la confianza transatlántica y ha repercutido negativamente en la confianza de las organizaciones estadounidenses que operan en la UE; y que lo anterior se ve agravado aún más por la falta de recursos administrativos y judiciales de que disponen los ciudadanos de la UE de conformidad con el Derecho

estadounidense, sobre todo en el caso de actividades de vigilancia para fines de inteligencia;

Transferencias a terceros países con la decisión de adecuación

AC. Considerando que, con arreglo a la información revelada y a las conclusiones de la investigación realizada por la Comisión LIBE, las agencias de seguridad nacional de Nueva Zelanda y Canadá han participado en una vigilancia masiva a gran escala de comunicaciones electrónicas y han colaborado activamente con los Estados Unidos en el programa denominado «Five eyes», y pueden haber intercambiado recíprocamente datos personales de los ciudadanos europeos transferidos desde la UE;

AD. Considerando que las Decisiones 2013/65[1] y 2/2002 de la Comisión, de 20 de diciembre de 2001,[2] han confirmado el nivel adecuado de protección garantizado por las Leyes de Documentos Electrónicos y Protección de la Información Personal de Nueva Zelanda y de Canadá; considerando asimismo que las revelaciones anteriores también minan gravemente la confianza en los sistemas jurídicos de estos países en lo que respecta a la continuidad de la protección garantizada a los ciudadanos de la UE; y que la Comisión no ha examinado esta cuestión;

Transferencias basadas en cláusulas contractuales y otros instrumentos

AE. Considerando que la Directiva 95/46/CE prevé que las transferencias internacionales a un tercer país también puedan realizarse mediante instrumentos específicos en los cuales el responsable de tratamiento de datos aduce garantías adecuadas con respecto a la protección de la intimidad, los derechos fundamentales y las libertades de las personas y con respecto al ejercicio de los derechos correspondientes;

AF. Considerando que estas garantías pueden, en particular, resultar de cláusulas contractuales pertinentes;

AG. Considerando que la Directiva 95/46/CE faculta a la Comisión para decidir qué cláusulas contractuales tipo específicas ofrecen las garantías suficientes requeridas por la Directiva y considerando, sobre esta base, que la Comisión ha adoptado tres modelos de cláusulas contractuales tipo para transferencias a los responsables y encargados (y subencargados) del tratamiento de datos en terceros países;

AH. Considerando que las Decisiones de la Comisión en las que se establecen las cláusulas contractuales tipo estipulan que las autoridades competentes en los Estados miembros pueden ejercer sus competencias actuales para suspender el flujo de datos cuando se establezca que la ley a la que están sujetos el importador de datos o un subencargado les impone desviaciones de la ley de protección de datos aplicable que vayan más allá de las restricciones necesarias en una sociedad democrática, como se establece en el artículo 13 de la Directiva 95/46/CE, si tales exigencias pueden tener un importante efecto negativo sobre las garantías previstas por la ley de protección de datos aplicable y las cláusulas contractuales tipo, o si existe la probabilidad sustancial de que estas

[1] DO L 28 de 30.01.13, p. 12.
[2] DO L 2 de 04.01.02, p. 13.

cláusulas contractuales tipo contenidas en el anexo no se estén respetando, o no se respeten en el futuro, y la continuación de la transferencia provoque un riesgo inminente de daños graves para los interesados;

AI. Considerando que las autoridades nacionales de protección de datos han desarrollado normas empresariales vinculantes con el fin de facilitar las transferencias internacionales dentro de una corporación multinacional con unas garantías adecuadas por lo que se refiere a la protección de la intimidad y los derechos y libertades fundamentales de las personas y al ejercicio de los derechos correspondientes; y que, antes de que se puedan utilizar, las normas empresariales vinculantes deben ser autorizadas por las autoridades competentes de los Estados miembros una vez que estas últimas hayan evaluado su conformidad con la legislación en materia de protección de datos de la Unión;

Transferencias basadas en los acuerdos TFTP y PNR

AJ. Considerando que, en su Resolución de 23 de octubre de 2013, el Parlamento Europeo expresó su profunda preocupación por las revelaciones relativas a las actividades de la Agencia Nacional de Seguridad en lo que respecta al acceso directo a los mensajes de pagos financieros y datos relacionados, que constituirían una evidente infracción del Acuerdo, en concreto de su artículo 1;

AK. Considerando que el Parlamento Europeo pidió a la Comisión que suspendiera el Acuerdo y solicitó que toda la información y los documentos relevantes estuvieran disponibles inmediatamente para las deliberaciones del Parlamento;

AL. Considerando que, a raíz de las alegaciones publicadas en los medios de comunicación, la Comisión decidió iniciar consultas con Estados Unidos en virtud del artículo 19 del Acuerdo TFTP; considerando asimismo que, el 27 de noviembre de 2013, la comisaria Malmström informó a la Comisión LIBE de que, tras reunirse con las autoridades estadounidenses y en vista de las respuestas dadas por dichas autoridades en sus cartas y durante sus reuniones, la Comisión había decidido no proseguir con las consultas debido a que no existían elementos que demostrasen que el Gobierno de los Estados Unidos ha actuado de forma contraria a las disposiciones del Acuerdo, y a que los Estados Unidos han ofrecido garantías por escrito de que no se ha producido ninguna recopilación de datos directa contraria a las disposiciones del Acuerdo TFTP;

AM. Considerando que, durante la visita de la delegación LIBE a Washington de los días 28 a 31 de octubre de 2013, la delegación se reunió con el Departamento del Tesoro de Estados Unidos; que el Tesoro estadounidense declaró que, desde la entrada en vigor del Acuerdo TFTP, no había tenido acceso a los datos SWIFT en la UE, salvo en el marco del TFTP; que el Tesoro estadounidense rehusó comentar si otro organismo o departamento del Gobierno de los Estados Unidos había accedido a los datos SWIFT al margen del TFTP o si el Gobierno de los Estados Unidos conocía las actividades de vigilancia masiva de la Agencia Nacional de Seguridad; y que, el 18 de diciembre de 2013, Glenn Greenwald declaró ante la comisión de investigación de la Comisión LIBE que la Agencia Nacional de Seguridad y el Centro Gubernamental de Comunicaciones (GCHQ) habían tenido como objetivo las redes SWIFT;

AN. Considerando que, el 13 de noviembre de 2013, las autoridades belgas y neerlandesas de protección de datos decidieron realizar una investigación conjunta sobre la seguridad de las redes de pago SWIFT para determinar si era posible que terceros accediesen de forma ilegal o no autorizada a los datos bancarios de los ciudadanos europeos [1];

AO. Considerando que, con arreglo a la revisión conjunta del Acuerdo PNR entre la UE y los EE.UU., el Departamento de Seguridad del Territorio Nacional de los Estados Unidos efectuó 23 divulgaciones de datos PNR a la Agencia Nacional de Seguridad, tras un examen caso por caso, como apoyo de casos de antiterrorismo y en consonancia con los términos específicos del Acuerdo;

AP. Considerando que la revisión conjunta no menciona el hecho de que en caso de que se traten datos personales con fines de inteligencia, en virtud del Derecho estadounidense, los ciudadanos europeos no disponen de vía administrativa o judicial alguna para proteger sus derechos y de que las garantías constitucionales solo se conceden a los ciudadanos estadounidenses; considerando que esta falta de derechos administrativos y judiciales anula la protección de los ciudadanos de la UE establecida en el acuerdo PNR existente;

Transferencias basadas en el Acuerdo de asistencia judicial en materia penal entre la Unión Europea y los Estados Unidos

AQ. Considerando que el Acuerdo de asistencia judicial en materia penal entre la Unión Europea y los Estados Unidos, de 6 de junio de 2003[2], entró en vigor el 1 de febrero de 2010 y está diseñado para facilitar la cooperación entre la UE y los Estados Unidos para luchar contra la delincuencia de forma más efectiva, teniendo en la debida consideración los derechos de las personas y el Estado de Derecho;

Acuerdo marco sobre la protección de datos en el ámbito de la cooperación policial y judicial («acuerdo marco»)

AR. Considerando que la finalidad de este acuerdo general es establecer el marco jurídico para todas las transferencias de datos personales entre la UE y los EE.UU. con el único objetivo de evitar, investigar, descubrir y perseguir las infracciones penales, incluido el terrorismo, en el marco de la cooperación policial y judicial en materia penal; y que las negociaciones fueron autorizadas por el Consejo el 2 de diciembre de 2010;

AS. Considerando que este acuerdo debe proporcionar unos principios claros, precisos y jurídicamente vinculantes para el tratamiento de datos, y debe reconocer, en particular, el derecho de los ciudadanos de la UE al acceso, rectificación y cancelación de sus datos personales en los EE.UU., así como el derecho a un mecanismo de recurso administrativo y judicial eficaz para los ciudadanos europeos y a una supervisión independiente de las actividades de tratamiento de datos;

[1] http://www.privacycommission.be/fr/news/les-instances-europ%C3%A9ennes-charg%C3%A9es-de-contr%C3%B4ler-le-respect-de-la-vie-priv%C3%A9e-examinent-la
[2] DO L 181 de 19.7.2003, p. 25.

AT. Considerando que, en su Comunicación de 27 de noviembre de 2013, la Comisión indicó que el «acuerdo marco» desembocaría en un elevado nivel de protección para los ciudadanos a ambas orillas del Atlántico y reforzaría la confianza de los europeos en los intercambios de datos entre la UE y los EE.UU., constituyendo la base para desarrollar una mayor cooperación y asociación entre la UE y los EE.UU. en materia de seguridad;

AU. Considerando que las negociaciones sobre el acuerdo no han avanzado debido a la persistente negativa por parte del Gobierno de los EE.UU. de reconocer los derechos efectivos a recurso administrativo y judicial de los ciudadanos de la UE, así como a la intención de prever amplias excepciones a los principios de protección de datos contenidos en el acuerdo, como la limitación de la finalidad, la retención de datos o las transferencias ulteriores, ya sean a nivel nacional o en el extranjero;

Reforma de la protección de datos

AV. Considerando que el marco jurídico para la protección de datos de la UE está siendo actualmente revisado para establecer un sistema sólido, moderno, coherente y completo para todas las actividades de tratamiento de datos en la Unión; que, en enero de 2012, la Comisión presentó un paquete de propuestas legislativas: un Reglamento general de protección de datos[1], que sustituirá a la Directiva 95/46/CE y establecerá una legislación uniforme en toda la UE, y una Directiva[2] que instaurará un marco armonizado para todas las actividades de tratamiento de datos de las autoridades policiales y reducirá las actuales divergencias entre las legislaciones nacionales;

AW. Considerando que, el 21 de octubre de 2013, la Comisión LIBE aprobó sus informes legislativos sobre ambas propuestas y decidió iniciar negociaciones con el Consejo con el fin de que dichos instrumentos jurídicos sean adoptados durante la presente legislatura;

AX. Considerando que, si bien el Consejo Europeo de los días 24 y 25 de octubre de 2013 pidió la adopción oportuna de un marco general de protección de datos de la UE sólido para reforzar la confianza de los ciudadanos y las empresas en la economía digital, el Consejo no ha sido capaz de lograr un enfoque general por lo que se refiere al Reglamento y a la Directiva general de protección de datos[3];

Seguridad informática y computación en nube

AY. Considerando que su Resolución de 10 de diciembre[4] destaca el potencial económico del negocio de la computación en nube para el crecimiento y el empleo;

AZ. Considerando que el nivel de protección de datos en un entorno de computación en nube no debe ser inferior al requerido en cualquier otro contexto de tratamiento de datos; y que la legislación en materia de protección de datos de la UE, por su neutralidad tecnológica, ya se aplica plenamente a los servicios de computación en

[1] COM(2012)11 de 25.1.2012.
[2] COM(2012)10 de 25.1.2012.
[3] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf
[4] AT-0353/2013 PE 506.114v2.00.

nube que operan en la UE;

BA. Considerando que, en virtud de los acuerdos de servicios en nube con los principales proveedores estadounidenses de servicios en nube, las actividades de vigilancia masiva proporcionan a las agencias de inteligencia acceso a los datos personales almacenados por los ciudadanos europeos; que las autoridades de inteligencia estadounidenses han accedido a los datos personales almacenados en servidores ubicados en territorio estadounidense recurriendo a las redes internas de Yahoo y de Google[1]; que dichas actividades constituyen una violación de las obligaciones internacionales; y que no cabe excluir que las autoridades de inteligencia también hayan accedido a información almacenada en los servicios en nube por las autoridades públicas o empresas e instituciones de los Estados miembros;

Control democrático de los servicios de inteligencia

BB. Considerando que los servicios de inteligencia realizan una importante función, protegiendo a la sociedad democrática de las amenazas internas y externas; que, a tal efecto, se les otorgan poderes y capacidades especiales; y que dichos poderes se deben utilizar en el marco del Estado de Derecho, ya que, de otro modo, se arriesgan a perder legitimidad y minar la naturaleza democrática de la sociedad;

BC. Considerando que el alto nivel de confidencialidad consustancial a los servicios de inteligencia para evitar que se pongan en peligro las operaciones en curso, se revelen los modos de actuación o peligren las vidas de los agentes, obstaculizan la plena transparencia, el control público y un examen normal desde el punto de vista democrático o judicial;

BD. Considerando que los avances tecnológicos han propiciado una cooperación internacional cada vez mayor en materia de inteligencia, lo que también implica el intercambio de datos personales y, a menudo, difumina la frontera entre la inteligencia y las actividades de las fuerzas del orden;

BE. Considerando que la mayoría de los mecanismos y organismos de vigilancia nacional existentes se establecieron y modernizaron en los años noventa del siglo pasado y no han sido adaptados necesariamente a los rápidos avances tecnológicos de la última década;

BF. Considerando que la vigilancia democrática de las actividades de inteligencia aún se realiza a nivel nacional, a pesar del creciente intercambio de información entre los Estados miembros de la UE y entre los Estados miembros y terceros países; considerando que existe una brecha cada vez mayor entre el nivel de cooperación internacional, por una parte, y las capacidades de vigilancia limitadas al nivel nacional, por otra, lo que resulta en un control democrático insuficiente e ineficaz;

Principales conclusiones

1. Considera que las recientes revelaciones en la prensa por parte de denunciantes y

[1] The Washington Post, 31 de octubre de 2013.

periodistas, junto con las pruebas periciales proporcionadas durante esta consulta, han resultado ser una prueba convincente de la existencia de sistemas tecnológicamente muy avanzados, complejos y de amplio alcance diseñados por los servicios de inteligencia de los Estados Unidos y de algunos Estados miembros para recopilar, almacenar y analizar datos y metadatos de comunicación y localización de todos los ciudadanos en todo el mundo a una escala sin precedentes y de una manera indiscriminada y no basada en sospechas;

2. Señala en concreto aquellos programas de inteligencia de la Agencia Nacional de Seguridad estadounidense que permiten la vigilancia masiva de los ciudadanos europeos mediante el acceso directo a los servidores centrales de empresas estadounidenses líderes en Internet (programa PRISM), el análisis de contenido y metadatos (programa Xkeyscore), la elusión del cifrado en línea (BULLRUN), el acceso a redes informáticas y telefónicas y el acceso a los datos de localización, así como algunos sistemas de la agencia de inteligencia británica GCHQ, como por ejemplo su actividad preliminar de vigilancia (programa Tempora) y su programa de descifrado (Edgehill); cree que es probable que existan programas de naturaleza similar, aunque sea a una escala más limitada, en otros países de la UE como Francia (DGSE), Alemania (BND) y Suecia (FRA);

3. Toma nota de las presuntas actividades de «pirateo» o interceptación en los sistemas Belgacom de la agencia de inteligencia británica GCHQ; reitera la indicación de Belgacom de que no podía confirmar que las instituciones europeas estuvieran afectadas o fueran objetivo de actividades de piratería, y que el software malicioso utilizado era extremadamente complejo y hubo de requerir el uso de amplios recursos financieros y de personal para su desarrollo y uso que no estaban al alcance de entidades privadas o piratas informáticos;

4. Afirma que la confianza se ha visto profundamente afectada: la confianza entre ambos socios trasatlánticos, la confianza entre los Estados miembros de la UE, la confianza entre los ciudadanos y sus gobiernos, la confianza en el respeto del Estado de Derecho y la confianza en la seguridad de los servicios informáticos; cree que, para restablecer la confianza en todas estas dimensiones, se requiere urgentemente un plan integral;

5. Señala que varios gobiernos argumentan que estos programas de vigilancia masiva son necesarios para combatir el terrorismo; apoya sin reservas la lucha contra el terrorismo, pero cree firmemente que nunca puede constituir en sí misma una justificación para llevar a cabo programas de vigilancia masiva secretos, no selectivos y, en ocasiones, incluso ilegales; expresa, por lo tanto, su preocupación por lo que respecta a la legalidad, necesidad y proporcionalidad de estos programas;

6. Considera muy dudoso que una recopilación de datos de dicha magnitud solo se guíe por la lucha contra el terrorismo, ya que implica la recopilación de todos los datos posibles de todos los ciudadanos; señala, por lo tanto, la posible existencia de otros motivos poderosos, como el espionaje político y económico;

7. Cuestiona la compatibilidad de las actividades de espionaje económico masivo de algunos Estados miembros con el mercado interior y la legislación sobre competencia de la UE, consagrada en los títulos I y VII del Tratado de Funcionamiento de la Unión

Europea; reafirma el principio de cooperación leal contemplado en el artículo 4, apartado 3, del Tratado de la Unión Europea y el principio según el cual los Estados miembros «se abstendrán de toda medida que pueda poner en peligro la consecución de los objetivos de la Unión»;

8. Señala que los tratados internacionales y la legislación de la Unión Europea y de los Estados Unidos, así como los mecanismos de control nacional, no han conseguido establecer los controles y equilibrios necesarios y una rendición de cuentas democrática;

9. Condena enérgicamente la recopilación general, sistemática y extensa de datos personales de personas inocentes que, a menudo, incluyen información personal íntima; enfatiza que los sistemas de vigilancia masiva indiscriminada por parte de los servicios de inteligencia constituyen una seria injerencia con los derechos fundamentales de los ciudadanos; destaca que la intimidad no es un lujo, sino la piedra angular de una sociedad libre y democrática; señala, asimismo, que la vigilancia masiva posee efectos potencialmente graves en la libertad de prensa, pensamiento y expresión, así como un potencial significativo para el abuso de la información recogida contra adversarios políticos; enfatiza que estas actividades de vigilancia masiva parecen asimismo implicar acciones ilegales por parte de los servicios de inteligencia y plantean interrogantes por lo que se refiere a la extraterritorialidad de las legislaciones nacionales;

10. Considera que los programas de vigilancia constituyen un paso más hacia el establecimiento de un estado preventivo de pleno derecho, cambiando el paradigma establecido de Derecho penal en las sociedades democráticas y promocionando en su lugar una mezcla de actividades policiales y de inteligencia con garantías jurídicas difuminadas, que no responden con frecuencia al control y equilibrio democráticos y a los derechos fundamentales, especialmente la presunción de inocencia; recuerda, al respecto, la decisión del Tribunal Constitucional Federal alemán[1] sobre la prohibición del uso de redadas preventivas («präventive Rasterfahndung») a menos que existan pruebas de un peligro concreto para otros derechos de alto nivel protegidos jurídicamente, por lo que no basta una situación de amenaza general o tensiones internacionales para justificar dichas medidas;

11. Insiste en que las leyes, tratados y tribunales secretos atentan contra el Estado de Derecho; señala que ninguna sentencia de un tribunal y ninguna decisión de una autoridad administrativa de un estado no perteneciente a la UE que autorice, directa o indirectamente, actividades de vigilancia como las examinadas por la presente investigación puede ser reconocida o ejecutada automáticamente, sino que debe ser sometida individualmente a los procedimientos nacionales adecuados sobre reconocimiento y asistencia jurídica mutuos, incluidas las normas impuestas por los acuerdos bilaterales;

12. Señala que las inquietudes anteriormente mencionadas se ven acentuadas por los rápidos avances tecnológicos y sociales; considera que la escala del problema no tiene precedentes, dado que Internet y los dispositivos móviles son omnipresentes en la vida

[1] Nº 1 BvR 518/02 de 4 de abril de 2006.

cotidiana moderna («recursos informáticos ubicuos») y que el modelo de negocio de la mayoría de las empresas de Internet se basa en el tratamiento de datos personales de todo tipo que pone en riesgo la integridad de la persona;

13. Considera que es natural concluir, según enfatizan los expertos en tecnología que expusieron su opinión en la presente investigación, que en la fase actual de desarrollo tecnológico no es posible garantizar, ni a las instituciones públicas de la UE ni a sus ciudadanos, que su seguridad o intimidad informática estén protegidas de la intrusión de terceros países bien equipados o de las agencias de inteligencia de la UE («falta de seguridad informática al 100 %»); advierte que esta alarmante situación solo puede resolverse si los europeos están dispuestos a dedicar suficientes recursos, tanto humanos como financieros, a conservar la independencia y autonomía de Europa;

14. Rechaza enérgicamente la idea de que estos asuntos sean meramente una cuestión de seguridad nacional y, por lo tanto, de competencia exclusiva de los Estados miembros; recuerda una reciente sentencia del Tribunal de Justicia según la cual «si bien corresponde a los Estados miembros adoptar las medidas adecuadas para garantizar su seguridad interior y exterior, el mero hecho de que una resolución esté relacionada con la seguridad del Estado no puede entrañar la inaplicabilidad del Derecho de la Unión»[1]; recuerda, asimismo, que está en juego la protección de la intimidad de todos los ciudadanos europeos, así como la seguridad y fiabilidad de todas las redes de comunicación de la UE; cree, por lo tanto, que el debate y las acciones a nivel de la UE no solo son legítimos, sino que se trata de una cuestión de autonomía y soberanía de la UE;

15. Elogia los actuales debates, consultas y revisiones en relación con el objeto de la presente investigación en diversas partes del mundo; señala la Reforma Global de Vigilancia del Gobierno suscrita por las empresas de tecnología líderes mundiales, que exige cambios radicales en las leyes nacionales sobre vigilancia, incluida una prohibición internacional de recopilación de datos en bloque para ayudar a mantener la confianza del público en Internet; señala con gran interés las recomendaciones publicadas recientemente por el Grupo de Revisión del Presidente estadounidense sobre Inteligencia y Tecnologías de las Comunicaciones; insta enérgicamente a los gobiernos a que tengan en cuenta estas peticiones y recomendaciones y a que revisen sus marcos nacionales para los servicios de inteligencia con objeto de implantar las garantías y el control adecuados;

16. Elogia a las instituciones y expertos que han contribuido a esta investigación; lamenta el hecho de que varias autoridades de los Estados miembros se hayan negado a cooperar con la investigación que ha realizado el Parlamento Europeo en nombre de los ciudadanos; celebra la transparencia de varios congresistas y diputados de los parlamentos nacionales;

17. Es consciente de que en un periodo de tiempo tan limitado solo ha sido posible realizar una investigación preliminar de todos los asuntos planteados desde julio de 2013; reconoce tanto la escala de las revelaciones como su carácter continuo; adopta, por lo tanto, un enfoque prospectivo que consiste en un conjunto de propuestas específicas y

[1] Nº 1 BvR 518/02 de 4 de abril de 2006.

un mecanismo de seguimiento en la próxima legislatura que garantice que las conclusiones ocupan un lugar predominante en la agenda política de la UE;

18. Tiene intención de exigir un compromiso político firme a la Comisión Europea que se designará después de las elecciones de mayo de 2014 para con la aplicación de las propuestas y recomendaciones de la presente investigación; espera un compromiso adecuado de los candidatos en las próximas audiencias parlamentarias de los nuevos comisarios;

Recomendaciones

19. Pide a las autoridades estadounidenses y a los Estados miembros de la UE que prohíban las actividades generales de vigilancia masiva y el tratamiento en bloque de los datos personales;

20. Pide a determinados Estados miembros de la UE, incluidos el Reino Unido, Alemania, Francia, Suecia y los Países Bajos, que revisen, si es necesario, sus legislaciones nacionales y las prácticas por las que se rigen las actividades de los servicios de inteligencia con el fin de garantizar que cumplen con lo establecido en la Convención Europea de Derechos Humanos y con sus obligaciones en materia de derechos fundamentales por lo que se refiere a la protección de datos, la intimidad y la presunción de inocencia; en particular, y dados los amplios informes de los medios de comunicación que hacen referencia a la vigilancia masiva en el Reino Unido, subrayaría que debe revisarse el actual marco jurídico integrado por una «compleja interacción» entre tres actos legislativos diferentes (Ley de derechos humanos de 1998, Ley de Servicios de Inteligencia de 1994 y Ley de regulación de las facultades de investigación de 2000);

21. Solicita a los Estados miembros que se abstengan de aceptar datos de terceros países que hayan sido recopilados ilegalmente y de permitir actividades de vigilancia en su territorio por gobiernos o agencias de terceros países que sean ilegales en virtud de la legislación nacional o que no cumplan con las garantías jurídicas contempladas en los instrumentos internacionales o de la UE, incluida la protección de los derechos humanos en virtud del Tratado de la UE, del CEDH y de la Carta de los Derechos Fundamentales de la UE;

22. Pide a los Estados miembros que cumplan de inmediato con su obligación positiva, a tenor del Convenio Europeo de Derechos Humanos, de proteger a sus ciudadanos de la vigilancia contraria a los requisitos establecidos —incluso cuando su objetivo sea salvaguardar la seguridad nacional— llevada a cabo por terceros países y garanticen que el Estado de Derecho no se vea debilitado por la aplicación extraterritorial de la legislación de un tercer país;

23. Invita al Secretario General del Consejo de Europa a lanzar el procedimiento del artículo 52, en virtud del cual «si se lo solicita el Secretario General del Consejo de Europa, cualquier Alta Parte Contratante debe explicar cómo garantiza su legislación interna la eficaz implementación de cualquiera de las disposiciones del Convenio»;

24. Pide a los Estados miembros que emprendan acciones de inmediato, incluidas

acciones judiciales, contra el ataque a su soberanía y, por lo tanto, la violación del derecho internacional público general, perpetrado a través de programas de vigilancia masiva; pide asimismo a los Estados miembros de la UE que hagan uso de todas las medidas internacionales disponibles para defender los derechos fundamentales de los ciudadanos europeos, especialmente mediante la puesta en marcha del procedimiento de reclamación entre Estados en virtud del artículo 41 del Pacto Internacional de Derechos Civiles y Políticos (ICCPR);

25. Pide a los Estados Unidos que revisen sin demora su legislación para adecuarla al Derecho internacional, reconozcan el derecho a la intimidad y otros derechos de los ciudadanos europeos, proporcionen recursos jurisdiccionales para los ciudadanos de la UE y suscriban el Protocolo Adicional que permite las denuncias individuales en virtud del ICCPR;

26. Se opone firmemente a cualquier conclusión de un protocolo o directriz adicional al Convenio del Consejo de Europa sobre Ciberdelincuencia (Convenio de Budapest) en lo concerniente al acceso transfronterizo a los datos informáticos almacenados, que podría suponer la legitimación del acceso por parte de los servicios de inteligencia a los datos almacenados en otra jurisdicción sin su autorización y sin el uso de los instrumentos de asistencia judicial mutua existentes, dado que ello podría resultar en el acceso remoto sin restricciones por parte de las autoridades policiales a servidores y ordenadores ubicados en otras jurisdicciones e iría en contra del Convenio nº 108 del Consejo de Europa;

27. Pide a la Comisión que, antes de julio de 2014, efectúe una evaluación de la aplicabilidad del Reglamento (CE) nº 2271/96 a los conflictos de legislaciones en las transferencias de datos personales;

Transferencias internacionales de datos

Marco jurídico de protección de datos y principio de puerto seguro de los Estados Unidos

28. Señala que las empresas que han sido señaladas por los medios de comunicación por su participación en las operaciones de vigilancia masiva a gran escala de individuos europeos por parte de la Agencia Nacional de Seguridad de los EE.UU. son empresas que han autocertificado su adhesión al principio de puerto seguro, y que el puerto seguro es el instrumento legal utilizado para la transferencia de datos personales de la Unión Europea a los Estados Unidos (Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); expresa su preocupación por el hecho de que estas organizaciones hayan admitido que no cifran ni la información ni las comunicaciones que fluyen entre sus centros de datos, lo cual permite a los servicios de inteligencia interceptar información[1];

29. Considera que el acceso a gran escala de las agencias de inteligencia de los EE.UU. a los datos personales de la UE procesados en virtud del principio de puerto seguro no cumple *per se* los criterios de exención en materia de seguridad nacional;

[1] The Washington Post, 31 de octubre de 2013.

30. Opina que, en vista de que los principios de puerto seguro no proporcionan una protección adecuada a los ciudadanos europeos en las circunstancias actuales, estas transferencias deben realizarse mediante otros instrumentos, como cláusulas contractuales o normas empresariales vinculantes que establezcan garantías y protecciones específicas;

31. Pide a la Comisión que presente medidas que prevean la suspensión inmediata de la Decisión 520/2000 de la Comisión, que establecía la adecuación de los principios de puerto seguro relativos a la protección de la intimidad, y de las preguntas más frecuentes relacionadas emitidas por el Departamento de Comercio de los Estados Unidos;

32. Pide a las autoridades competentes de los Estados miembros, esto es, a las autoridades responsables de la protección de datos, que utilicen sus poderes actuales y suspendan de inmediato el flujo de datos a cualquier organización que haya autocertificado su adhesión a los principios de puerto seguro de los EE.UU. y que exijan que dichos flujos de datos solo se efectúen mediante otros instrumentos, siempre que contengan las garantías y protecciones necesarias con respecto a la protección de la intimidad y los derechos y libertades fundamentales de las personas;

33. Invita a la Comisión a que presente, antes de junio de 2014, una evaluación completa del marco aplicable en materia de protección de la intimidad que cubra las actividades comerciales, policiales y de inteligencia en respuesta a las divergencias que presentan los sistemas jurídicos de la UE y de los EE.UU. en materia de protección de datos personales;

Transferencias a otros terceros países con la decisión de adecuación

34. Recuerda que la Directiva 95/46/CE estipula que las transferencias de datos personales a un tercer país solo pueden realizarse si, sin perjuicio del cumplimiento de las disposiciones nacionales adoptadas en virtud de las otras disposiciones de la Directiva, el tercer país en cuestión garantiza un nivel adecuado de protección, siendo la finalidad de dicha disposición garantizar la continuidad de la protección conferida por la normativa en materia de protección de datos de la UE, cuando se transfieran datos personales fuera de la UE;

35. Recuerda que la Directiva 95/46/CE prevé que la adecuación del nivel de protección conferido por un tercer país debe ser evaluado a la luz de todas las circunstancias que rodean a la operación de transferencia de los datos o al conjunto de las operaciones de transferencia de datos; recuerda asimismo que dicha Directiva también dota a la Comisión de competencias de ejecución para declarar que un tercer país garantiza un nivel adecuado de protección a la luz de los criterios establecidos por la Directiva 95/46/CE, mientras que la Directiva 95/46/CE también faculta a la Comisión a declarar que un tercer país no garantiza un adecuado nivel de protección;

36. Recuerda que, en este último caso, los Estados miembros deben adoptar las medidas necesarias para evitar cualquier transferencia de datos del mismo tipo al tercer país en cuestión, y que la Comisión debe entablar negociaciones con el objetivo de resolver la situación;

37. Pide a la Comisión y a los Estados miembros que evalúen sin demora si el nivel de protección adecuado de las Leyes de Documentos Electrónicos y Protección de la Información Personal de Nueva Zelanda y de Canadá, según se declara en las Decisiones de la Comisión 2013/651 y 2/2002, de 20 de diciembre de 2001, se ha visto afectado por la intervención de sus agencias nacionales de inteligencia en la vigilancia masiva de ciudadanos de la UE y, si procede, que tomen las medidas apropiadas para suspender o revertir las decisiones de adecuación; espera que la Comisión informe al Parlamento Europeo de sus conclusiones sobre los países anteriormente mencionados para diciembre de 2014, a más tardar;

Transferencias basadas en cláusulas contractuales y otros instrumentos

38. Recuerda que las autoridades nacionales de protección de datos han indicado que ni las cláusulas contractuales tipo ni las normas empresariales vinculantes fueron redactadas teniendo en cuenta las situaciones de acceso a datos personales a efectos de vigilancia masiva, y que dicho acceso no se ajustaría a las cláusulas de excepción de las cláusulas contractuales o normas empresariales vinculantes que se refieren a las excepciones para un interés legítimo en una sociedad democrática y cuando resulte necesario y proporcionado;

39. Pide a los Estados miembros que prohíban o suspendan los flujos de datos a terceros países con arreglo a las cláusulas contractuales tipo, las cláusulas contractuales o las normas empresariales vinculantes autorizadas por las autoridades nacionales competentes cuando se determine que la ley a la que está sometido el importador de los datos le impone requisitos que van más allá de las restricciones necesarias en una sociedad democrática y que pueden tener un importante efecto negativo sobre las garantías previstas por la ley de protección de datos aplicable y las cláusulas contractuales tipo, o cuando la continuación de la transferencia pueda provocar un riesgo inminente de daños graves para los interesados;

40. Pide al Grupo de Trabajo del Artículo 29 que emita directrices y recomendaciones sobre las garantías y protecciones que deben contener los instrumentos contractuales para las transferencias internacionales de datos personales en la UE con el fin de garantizar la protección de la intimidad, los derechos fundamentales y las libertados de las personas, teniendo en cuenta especialmente las leyes de terceros países sobre inteligencia y seguridad nacional y la participación de las empresas que reciben los datos en un tercer país en las actividades de vigilancia masiva por parte de las agencias de inteligencia de un tercer país;

41. Pide a la Comisión que examine las cláusulas contractuales tipo que ha establecido con el fin de evaluar si ofrecen la protección necesaria en lo que respecta al acceso a los datos personales transferidos en virtud de las cláusulas con fines de inteligencia y, si procede, que las revise;

Transferencias basadas en el Acuerdo de Asistencia Judicial

42. Pide a la Comisión que realice, antes de que finalice 2014, una evaluación en

[1] DO L 28 de 30.01.13, p. 12.

profundidad del Acuerdo de Asistencia Judicial, de conformidad con su artículo 17, con el fin de verificar su implementación práctica y, en particular, de comprobar si los Estados Unidos han hecho un uso efectivo del mismo para obtener información o pruebas en la UE y si se ha eludido el Acuerdo para adquirir la información directamente en la UE, así como que evalúe el impacto en los derechos fundamentales de los ciudadanos; considera que dicha evaluación no debe hacer referencia únicamente a las declaraciones oficiales estadounidenses como base suficiente para el análisis sino basarse en evaluaciones específicas de la UE; estima que dicha revisión en profundidad debe abordar igualmente las consecuencias de la aplicación de la arquitectura constitucional de la Unión a este instrumento para adecuarlo al Derecho de la Unión, teniendo en cuenta en particular su protocolo 36 y su artículo 10 y la declaración 50 relativa a este protocolo;

Asistencia mutua en materia penal en la UE

43. Pide al Consejo y a la Comisión que informen al Parlamento sobre el uso real que hacen los Estados miembros del Convenio sobre Asistencia Mutua en materia penal entre los Estados miembros, en particular su título III sobre la interceptación de telecomunicaciones; pide a la Comisión que, de conformidad con la declaración 50, presente una propuesta relativa al protocolo 36, como se solicitó, antes del fin de 2014 a fin de adaptarlo al marco del Tratado de Lisboa;

Transferencias basadas en los acuerdos TFTP y PNR

44. Opina que la información proporcionada por la Comisión Europea y el Tesoro estadounidense no aclara si las agencias de inteligencia estadounidenses tienen acceso a los mensajes financieros SWIFT en la UE mediante la interceptación de las redes SWIFT o los sistemas operativos y las redes de comunicación de los bancos, por sí solas o en colaboración con agencias de inteligencia nacionales de la UE y sin recurrir a los canales bilaterales existentes para la asistencia y la cooperación judiciales mutuas;

45. Reitera su Resolución de 23 de octubre de 2013 y pide a la Comisión que suspenda el acuerdo TFTP;

46. Pide a la Comisión Europea que intervenga ante la preocupación por el hecho de que tres de los principales sistemas de reserva informáticos utilizados por las compañías aéreas en todo el mundo se encuentren en los Estados Unidos y de que los datos PNR estén almacenados en sistemas en nube que operan en territorio estadounidense y en virtud de la legislación estadounidense, que carece de la adecuada protección de los datos;

Acuerdo marco sobre la protección de datos en el ámbito de la cooperación policial y judicial («acuerdo marco»)

47. Considera que una solución satisfactoria en virtud del «acuerdo marco» constituye una condición previa para la completa recuperación de la confianza entre los socios trasatlánticos;

48. Pide la inmediata reanudación de las negociaciones con los Estados Unidos en relación con el «acuerdo marco», que debe prever derechos claros para los ciudadanos europeos y recursos administrativos y judiciales eficaces y aplicables en los Estados Unidos, sin discriminación;

49. Pide a la Comisión y al Consejo que no inicien ningún nuevo acuerdo sectorial ni disposiciones para la transferencia de datos personales con fines policiales hasta que el «acuerdo marco» no haya entrado en vigor;

50. Insta a la Comisión a dar cuentas en detalle de los diversos puntos del mandato de negociación y de la situación actual para abril de 2014;

Reforma de la protección de datos

51. Pide a la Presidencia del Consejo y a la mayoría de los Estados miembros que están a favor de un elevado nivel de protección de datos que muestren un sentido de liderazgo y responsabilidad y aceleren su labor en relación con el Paquete de Protección de Datos completo para permitir su adopción en 2014, de modo que los ciudadanos de la UE puedan disfrutar de una mejor protección en un futuro muy cercano;

52. Destaca que tanto el Reglamento de Protección de Datos como la Directiva sobre Protección de Datos son necesarios para proteger los derechos fundamentales de las personas y, por lo tanto, deben tratarse como un paquete que se ha de adoptar de manera simultánea, con el fin de garantizar que todas las actividades de tratamiento de datos en la UE ofrecen un elevado nivel de protección en todas las circunstancias;

Computación en nube

53. Señala que la confianza en la computación en nube estadounidense y en sus proveedores se ha visto afectada negativamente por las prácticas arriba indicadas; enfatiza, por tanto, que el desarrollo de servicios en nube europeos constituye un elemento esencial para el crecimiento y el empleo y para para la confianza en los servicios y proveedores de computación en nube, así como para garantizar un buen nivel de protección de los datos personales;

54. Reitera su gran preocupación por la divulgación directa y obligatoria de información y datos personales de la UE tratados en el marco de contratos de servicio en nube a autoridades de terceros países por prestadores de servicios en nube sujetos a la legislación de un tercer país o que utilicen servidores de almacenamiento ubicados en terceros países y por el acceso remoto directo a los datos e información personales tratados por las autoridades policiales y los servicios de inteligencia de terceros países;

55. Deplora que este acceso se consiga habitualmente por medio de la aplicación directa por parte de las autoridades de terceros países de sus propias normas jurídicas sin utilizar los instrumentos internacionales establecidos para la cooperación judicial, como los acuerdos de asistencia judicial mutua u otras formas de cooperación judicial;

56. Pide a la Comisión y a los Estados miembros que aceleren el establecimiento de la Asociación Europea de Computación en Nube;

57. Recuerda 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;

Acuerdo de Asociación Transatlántica para el Comercio y la Inversión (ATCI)

58. Reconoce que la UE y los Estados Unidos están negociando un Acuerdo de Asociación Transatlántica para el Comercio y la Inversión, una herramienta de importancia estratégica capital para crear más crecimiento económico y para que tanto la UE como loso Estados Unidos puedan establecer normas mundiales de reglamentación en el futuro;

59. Hace especial hincapié, dada la importancia de la economía digital en la relación y en la causa de la recuperación de la confianza entre la UE y los Estados Unidos, en que el Parlamento Europeo únicamente dará su consentimiento a la versión final del ATCI en caso de que dicho acuerdo respete los derechos fundamentales reconocidos por la Carta de la UE, y en que la protección de la intimidad de las personas en relación con el procesamiento y la divulgación de datos personales deben seguir rigiéndose por el artículo XIV del AGCS;

Control democrático de los servicios de inteligencia

60. Insiste en que, a pesar de que el control de las actividades de los servicios de inteligencia tiene que estar basado tanto en la legitimidad democrática (marco jurídico sólido, autorización previa y verificación posterior) como en una capacidad y unos conocimientos técnicos adecuados, la mayoría de los organismos actuales de control de la UE y de los Estados Unidos carecen de ambos, en especial de capacidad técnica;

61. Invita, al igual que en el caso de Echelon, a todos los parlamentos nacionales que aún no lo hayan hecho a que establezcan un control coherente de las actividades de inteligencia por parte de parlamentarios u organismos especializados con potestad legal de investigación; hace un llamamiento a los parlamentos nacionales para que garanticen que dichos comités u organismos de control tengan recursos, conocimientos técnicos y medios legales suficientes para que puedan controlar con eficacia los servicios de inteligencia;

62. Pide el establecimiento de un grupo de alto nivel para fortalecer la cooperación en el ámbito de la inteligencia a nivel comunitario, combinado con un mecanismo de control adecuado que garantice tanto la legitimidad democrática como una capacidad técnica adecuada; insiste en que el grupo de alto nivel debe cooperar estrechamente con los parlamentos nacionales con el fin de proponer más medidas para aumentar la colaboración en las cuestiones de control en la UE;

63. Pide a este grupo de alto nivel que defina las directrices o estándares mínimos europeos por lo que se refiere al control (ex ante y ex post) de los servicios de inteligencia sobre la base de los códigos de buenas prácticas y recomendaciones existentes de organismos internacionales (Naciones Unidas, Consejo de Europa);

64. Pide que el grupo de alto nivel establezca límites estrictos en cuanto a la duración de cualquier vigilancia ordenada, a no ser que la continuación de la misma sea

debidamente justificada por las autoridades de control;

65. Solicita al grupo de alto nivel que desarrolle criterios de mejor transparencia a partir del principio general de acceso a la información y de los llamados «Principios de Tshwane»[1];

66. Tiene intención de organizar una conferencia con los organismos nacionales de control, ya sean parlamentarios o independientes, a finales de 2014;

67. Solicita a los Estados miembros que elaboren un código de buenas prácticas para mejorar el acceso de sus organismos de control a la información sobre las actividades de inteligencia (que incluya información clasificada e información de otros servicios) y establezcan la facultad para llevar a cabo visitas *in situ*, un conjunto sólido de poderes de interrogación, recursos y conocimientos técnicos adecuados, independencia estricta frente a sus respectivos gobiernos y la obligación de informar a sus parlamentos respectivos;

68. Pide a los Estados miembros que desarrollen mecanismos de cooperación entre los organismos de control, en especial dentro de la ENNIR (European Network of National Intelligence Reviewers);

69. Insta a la Comisión a presentar antes de septiembre de 2014 una propuesta de marco legal para las actividades del Centro de Análisis de Inteligencia de la UE (IntCen), así como un mecanismo de control adecuado adaptado a sus actividades que incluya una rendición regular de cuentas al Parlamento Europeo;

70. Solicita a la Comisión que presente antes de septiembre de 2014 una propuesta de procedimiento de habilitación de seguridad comunitario para todos los funcionarios de la UE, ya que el sistema actual, que se basa en la habilitación de seguridad del Estado miembro del que se tiene nacionalidad, tiene unos requisitos y una duración de los procedimientos distintos dentro de los sistemas nacionales, lo que conlleva un tratamiento diferente de los diputados y de su personal dependiendo de su nacionalidad;

71. Recuerda las disposiciones del Acuerdo interinstitucional entre el Parlamento Europeo y el Consejo sobre la transmisión al Parlamento Europeo y la gestión por el mismo de la información clasificada en posesión del Consejo sobre asuntos distintos de los pertenecientes al ámbito de la política exterior y de seguridad común, que debe emplearse para mejorar el control a nivel comunitario;

Agencias de la UE

72. Hace un llamamiento a la Autoridad Común de Control de Europol, junto con las agencias nacionales de protección de datos, para que lleven a cabo una inspección conjunta antes de que finalice 2014 con el fin de determinar si la información y los datos personales compartidos por Europol han sido obtenidos de forma legal por las

[1] The Global Principles on National Security and the Right to Information [Los principios mundiales relativos a la seguridad nacional y el derecho a la información], junio de 2013.

autoridades nacionales, especialmente si la información o los datos fueron obtenidos inicialmente por los servicios de inteligencia en la UE o en terceros países, y si están en vigor medidas adecuadas para evitar el uso y la divulgación de dicha información o datos;

73. Hace un llamamiento a Europol para que solicite a las autoridades competentes de los Estados miembros, de acuerdo con sus competencias, que emprendan investigaciones sobre ciberdelincuencia y ataques cibernéticos cometidos por gobiernos o entes privados en el transcurso de las actividades objeto de examen;

Libertad de expresión

74. Expresa una gran preocupación por las amenazas que se ciernen sobre la libertad de prensa y el efecto amedrentador de la intimidación de las autoridades del Estado sobre los periodistas, en especial en lo que concierne a la protección de la confidencialidad de las fuentes periodísticas; reitera los llamamientos realizados en su Resolución de 21 de mayo de 2013 sobre la «Carta de la UE: Normas para la libertad de los medios de comunicación en la UE»;

75. Considera que la detención de David Miranda y la incautación del material que obraba en su poder de conformidad con el apéndice 7 de la Ley antiterrorista de 2000 (y también el requerimiento a *The Guardian* para que destruyese o entregase el material) suponen una injerencia en el derecho a la libertad de expresión reconocida en el artículo 10 de la CEDH y el artículo 11 de la Carta de la UE;

76. Hace un llamamiento a la Comisión para que presente una propuesta de marco general para la protección de informantes en la UE, con especial atención a las especificidades de la denuncia de irregularidades en el ámbito de los servicios de inteligencia, para las cuales las disposiciones sobre denuncia de irregularidades en el ámbito financiero pueden resultar insuficientes, y que incluya garantías sólidas de inmunidad;

Seguridad informática de la UE

77. Señala que los recientes sucesos demuestran claramente la grave vulnerabilidad de la UE, y en particular de sus instituciones, Gobiernos y Parlamentos nacionales, grandes empresas europeas, e infraestructuras y redes informáticas europeas, ante sofisticados ataques por medio de complejos programas de software; incide en que estos ataques precisan de tales recursos humanos y financieros que probablemente tengan su origen en entes estatales que trabajan en nombre de gobiernos extranjeros o incluso de determinados gobiernos nacionales de la UE que los respaldan; en este contexto, considera el caso de la piratería o intercepción de la empresa de telecomunicaciones Belgacom como un preocupante ejemplo de un ataque contra la capacidad informática de la UE;

78. Opina que las revelaciones sobre vigilancia masiva que han iniciado esta crisis pueden emplearse como una oportunidad para que Europa tome la iniciativa y cree una capacidad autónoma de recursos informáticos fundamentales a medio plazo; hace un llamamiento a la Comisión y a los Estados miembros para que utilicen los contratos públicos como palanca para respaldar dicha capacidad de recursos en la UE,

convirtiendo los estándares de seguridad e intimidad de la UE en un requisito fundamental en los contratos públicos de bienes y servicios informáticos;

79. Demuestra su gran preocupación por los indicios de que servicios de inteligencia extranjeros han intentado rebajar los estándares de seguridad informática e instalar puertas traseras en un amplio espectro de sistemas informáticos;

80. Hace un llamamiento a los Estados miembros, la Comisión, el Consejo y el Consejo Europeo para que hagan frente a la peligrosa falta de autonomía de la UE en lo que respecta a herramientas, empresas y proveedores informáticos (hardware, software, servicios y redes) y capacidad criptográfica y de cifrado;

81. Pide a la Comisión, a los organismos de normalización y a ENISA que desarrollen antes de septiembre de 2014 estándares y directrices mínimos de seguridad e intimidad para los sistemas, redes y servicios informáticos, incluidos servicios de computación en nube, con el fin de proteger mejor los datos personales de los ciudadanos de la UE; cree que dichos estándares deben fijarse en un proceso abierto y democrático que no esté dirigido por un solo país, entidad o empresa multinacional; opina que, aunque hay que tener en cuenta los motivos legítimos de preocupación de las agencias de policía e inteligencia para respaldar la lucha contra el terrorismo, no deben conllevar un socavamiento general de la fiabilidad de todos los sistemas informáticos;

82. Señala que tanto las empresas de telecomunicaciones como los reguladores nacionales y comunitarios de las telecomunicaciones han descuidado la seguridad informática de sus usuarios y clientes; pide a la Comisión que emplee todos sus poderes actuales de conformidad con la Directiva marco sobre telecomunicaciones e intimidad electrónica para fortalecer la protección de la confidencialidad de la comunicación, adoptando medidas que garanticen que los terminales sean compatibles con el derecho de los usuarios a controlar y proteger sus datos personales, y para garantizar un alto nivel de seguridad de las redes y servicios de telecomunicaciones, asimismo mediante la exigencia de un cifrado avanzado de las comunicaciones;

83. Respalda la estrategia cibernética de la UE, pero considera que no abarca todas las amenazas posibles y debe ampliarse para que incluya comportamientos estatales maliciosos;

84. Pide a la Comisión que presente a lo sumo antes de enero de 2015 un plan de acción para desarrollar la independencia de la UE en el sector informático que incluya un planteamiento más coherente para fomentar la capacidad informática de la UE (sistemas informáticos, equipos, servicios, computación en nube, cifrado y anonimización, entre otros aspectos) y para proteger toda la infraestructura informática vital (incluido todo lo referente a propiedad y vulnerabilidad);

85. Pide a la Comisión, en el marco del siguiente programa de trabajo del programa Horizonte 2020, que evalúe si deben destinarse más recursos al fomento de la investigación, desarrollo, innovación y formación en Europa en el ámbito de las tecnologías de la información, y, en particular, en tecnologías e infraestructuras de protección de la intimidad, criptología, computación segura, soluciones de seguridad de código abierto y sociedad de la información;

86. Solicita a la Comisión que planifique las responsabilidades actuales y examine antes de junio de 2014 la necesidad de un mandato más amplio, mejor coordinación o recursos y capacidad técnica adicionales para el Centro de Ciberdelincuencia de Europol, ENISA, CERT-EU y el SEPD, con el fin de que sean más eficaces en la investigación de delitos informáticos en la UE y en la realización (o ayuda a la realización por parte de Estados miembros y organismos de la UE) de investigaciones técnicas *in situ* de delitos informáticos de gran calado;

87. Considera necesario que la UE reciba ayuda de una Academia de Tecnologías de la Información de la UE que reúna a los mejores expertos europeos de todos los campos relacionados y se encargue de asesorar científicamente a todas las instituciones y organismos correspondientes de la UE sobre tecnologías de la información, incluidas estrategias relacionadas con la seguridad; como primer paso, pide a la Comisión que establezca un panel de expertos científicos independiente;

88. Hace un llamamiento a la Secretaría General del Parlamento Europeo para que lleve a cabo antes de septiembre de 2014, como máximo, una profunda revisión y evaluación de la fiabilidad de la seguridad informática del Parlamento Europeo centrada en: medios presupuestarios, recursos de personal, capacidad técnica, organización interna y todos los elementos oportunos para conseguir un elevado nivel de seguridad de los sistemas informáticos del Parlamento Europeo; cree que dicha evaluación debe aportar un análisis informativo y recomendaciones sobre los siguientes asuntos:

- la necesidad de ensayos de penetración y auditorías de seguridad independientes, rigurosos y periódicos, con la selección de expertos de seguridad externos que garanticen la transparencia y sus credenciales frente a terceros países o cualquier tipo de intereses creados;

- la inclusión en los procedimientos de licitación de nuevos sistemas informáticos de requisitos informáticos específicos que incluyan la posibilidad de un requisito de software de código abierto como condición de compra;

- la lista de empresas estadounidenses que trabajan con el Parlamento Europeo en los campos de la informática y las telecomunicaciones, a raíz de las revelaciones acerca de los contratos de la NSA con empresas como RSA, cuyos productos emplea el Parlamento Europeo para supuestamente proteger el acceso remoto a sus datos por parte de diputados y personal;

- la fiabilidad y resistencia del software comercial de terceros utilizado por las instituciones de la UE en sus sistemas informáticos en lo que respecta a la intromisión y penetración de las autoridades policiales y de inteligencia de la UE o de terceros países;

- el uso de más sistemas de código abierto y menos sistemas comerciales genéricos;

- el impacto del aumento del uso de herramientas móviles (*smartphones* o tabletas, ya sean profesionales o personales) y sus efectos en la seguridad

informática del sistema;

- la seguridad de la comunicación entre los diferentes lugares de trabajo del Parlamento Europeo y de los sistemas informáticos utilizados en él;

- el uso y la ubicación de los servidores y centros informáticos de los sistemas del Parlamento Europeo y las consecuencias para la seguridad e integridad de los sistemas;

- la puesta en práctica real de las normas existentes sobre violaciones de seguridad y su inmediata notificación a las autoridades competentes por parte de los proveedores de redes de telecomunicaciones públicas;

- el uso de almacenamiento en nube por parte del Parlamento Europeo, lo que incluye el tipo de datos que se almacenan en la nube, cómo se protege el contenido y se accede a él, dónde se ubica la nube, y cuál es el régimen legal de protección de datos aplicable;

- un plan que permita el uso de más tecnologías criptográficas, especialmente cifrado autentificado de extremo a extremo para todos los servicios informáticos y de comunicaciones como la computación en nube, el correo electrónico, la mensajería instantánea y la telefonía.

- el uso de la firma electrónica en el correo electrónico;

- un análisis de las ventajas de emplear GNU Privacy Guard como estándar de cifrado predeterminado para los correos electrónicos que permitiría al mismo tiempo el uso de firmas digitales;

- la posibilidad de establecer un servicio seguro de mensajería instantánea dentro del Parlamento Europeo que garantice la seguridad en la comunicación y en el que el servidor solo vea contenido cifrado;

89. Hace un llamamiento a todas las instituciones y agencias de la UE para que lleven a cabo un ejercicio similar antes de diciembre de 2014, en especial al Consejo Europeo, el Consejo, el Servicio de Acción Exterior (incluidas las delegaciones de la UE), la Comisión, el Tribunal de Justicia Europeo y el Banco Central Europeo; invita a los Estados miembros a efectuar evaluaciones similares;

90. Destaca que, en lo que concierne a la acción exterior de la UE, deben llevarse a cabo evaluaciones de las necesidades presupuestarias y tomarse las primeras medidas sin demora en el caso del Servicio de Acción Exterior Europeo (SEAE) y que deben destinarse los fondos necesarios en el proyecto de presupuesto para 2015;

91. Opina que los sistemas informáticos a gran escala utilizados en el área de libertad, seguridad y justicia, como el Sistema de Información de Schengen II, el Sistema de Información de Visados, Eurodac y otros posibles sistemas futuros, tienen que desarrollarse y ponerse en funcionamiento de tal forma que garanticen que los datos no están en peligro como resultado de las solicitudes de los Estados Unidos de acuerdo

con la Ley Patriótica; pide a eu-LISA que informe al Parlamento sobre la fiabilidad de los sistemas utilizados antes de finales de 2014;

92. Pide a la Comisión y al SEAE que emprendan acciones a nivel internacional, especialmente en las Naciones Unidas y en colaboración con socios interesados (como Brasil) y que pongan en práctica una estrategia comunitaria para la gobernanza democrática de Internet con el fin de evitar influencias indebidas sobre las actividades de ICANN e IANA por parte de entidades, empresas o países individuales garantizando una representación adecuada de todas las partes interesadas en estos organismos;

93. Pide que se reconsidere la arquitectura general de Internet en términos de almacenamiento y flujos de datos, para conseguir una mayor transparencia y minimización de los datos y un menor almacenamiento masivo centralizado de los datos en bruto, y también para evitar una redirección innecesaria del tráfico a través del territorio de países que no cumplen los estándares básicos de derechos fundamentales, protección de datos e intimidad;

94. Hace un llamamiento a los Estados miembros, en colaboración con ENISA, el Centro de Ciberdelincuencia de Europol, CERT y las autoridades nacionales de protección de datos y unidades de ciberdelincuencia para que inicien una campaña de educación y concienciación con el fin de permitir que los ciudadanos estén más informados a la hora de elegir los datos personales que quieren confiar a Internet y cómo se los puede proteger mejor, como, por ejemplo, a través de «higiene digital», cifrado y computación en nube segura, haciendo pleno uso de la plataforma de información de interés público incluida en la Directiva de servicio universal;

95. Pide a la Comisión que, antes de septiembre de 2014, evalúe las posibilidades de alentar a los fabricantes de software y hardware para que introduzcan más seguridad e intimidad a través de características predeterminadas en sus productos, como la posibilidad de introducir responsabilidad legal por parte de los fabricantes por la omisión de parchear vulnerabilidades conocidas o la instalación de puertas traseras secretas, o desincentivar la recogida indebida y desproporcionada de datos personales masivos, y, si procede, que presente propuestas legislativas;

Recuperación de la confianza

96. Cree que la investigación ha mostrado la necesidad de que los Estados Unidos recuperen la confianza de sus socios, ya que se trata fundamentalmente de las actividades de las agencias de inteligencia de los Estados Unidos;

97. Señala que la crisis de confianza generada se extiende a los siguientes puntos:

– el espíritu de cooperación dentro de la UE, ya que algunas actividades de los servicios de inteligencia nacionales pueden poner en peligro la consecución de los objetivos de la Unión;

– los ciudadanos, que se dan cuenta de que no solo terceros países o multinacionales, sino también su propio gobierno, pueden estar espiándolos;

– el respeto a la ley y la credibilidad de las salvaguardas democráticas en una sociedad digital;

Entre la UE y Estados Unidos

98. Recuerda la importante asociación estratégica e histórica entre los Estados miembros de la UE y los Estados Unidos, basada en una creencia común en la democracia, el Estado de Derecho y los derechos fundamentales;

99. Cree que la vigilancia masiva de los ciudadanos y el espionaje de los líderes políticos por parte de los Estados Unidos ha causado serios daños en las relaciones entre la UE y los Estados Unidos y ha tenido un impacto negativo en la confianza en las entidades estadounidenses que actúan en la UE; considera que eso se ve agravado aún más por la falta de vías de recurso administrativo y judicial en virtud del Derecho estadounidense para los ciudadanos europeos, sobre todo en el caso de actividades de vigilancia para fines de inteligencia;

100. Reconoce, a la luz de los retos mundiales a los que se enfrentan la UE y los Estados Unidos, que el vínculo transatlántico tiene que fortalecerse más y que es vital que continúe la cooperación transatlántica en la lucha antiterrorista; insiste, sin embargo, en que los Estados Unidos deben tomar claras medidas para restablecer la confianza y volver a subrayar los valores básicos compartidos sobre los que se sustenta la asociación;

101. Está preparado para entablar el diálogo con sus homólogos estadounidenses para que en el actual debate público y parlamentario en los Estados Unidos sobre la reforma de la vigilancia y la reconsideración del control de la inteligencia se tengan en cuenta los derechos a la intimidad de los ciudadanos de la UE, se garanticen los mismos derechos de información y protección de la intimidad en los tribunales de Estados Unidos y deje de perpetuarse la actual discriminación;

102. Insiste en que deben emprenderse reformas necesarias y deben ofrecerse garantías efectivas a los europeos para que el uso de la vigilancia y el procesamiento de datos en el espionaje exterior estén limitados por condiciones especificadas claramente y vinculados a sospechas razonables o probables causas de actividades terroristas o criminales; destaca que este fin debe estar sujeto a un control judicial transparente;

103. Considera que nuestros socios estadounidenses deben enviar señales políticas para demostrar que los Estados Unidos distinguen entre aliados y enemigos;

104. Insta a la Comisión Europea y al Gobierno de los Estados Unidos a abordar, en el contexto de las negociaciones en curso sobre un acuerdo general entre la UE y Estados Unidos sobre el intercambio de datos con fines policiales, los derechos de información y compensación judicial de los ciudadanos de la UE, y a cerrar dichas negociaciones, de acuerdo con el compromiso adquirido en la cumbre de ministros de justicia e interior de la UE y Estados Unidos del 18 de noviembre de 2013, antes del verano de 2014;

105. Solicita a Estados Unidos que se adhiera a la Convención europea para la protección

de las personas en relación con el procesamiento automático de datos personales (convención 108), al igual que se adhirió a la Convención sobre ciberdelincuencia de 2001, para fortalecer la base legal común entre los aliados transatlánticos;

106. Hace un llamamiento a las instituciones de la UE para explorar las posibilidades de establecer un código de conducta con Estados Unidos que garantizase que no se lleven a cabo actividades de espionaje estadounidenses contra instituciones ni instalaciones de la UE;

Dentro de la Unión Europea

107. También cree que la implicación y actividades de algunos Estados miembros de la UE ha conducido a una pérdida de confianza; opina que únicamente mediante una total claridad en cuanto a los fines y medios de vigilancia, un debate público y, en última instancia, una revisión de la legislación que incluya un fortalecimiento de las funciones judiciales y parlamentarias de control se conseguirá restablecer la confianza perdida;

108. Es consciente de que algunos de los Estados miembros están llevando a cabo intercambios bilaterales con las autoridades de Estados Unidos sobre las acusaciones de espionaje, y que algunos de ellos han pactado (Reino Unido) o prevén pactar (Francia, Alemania) acuerdos antiespionaje; subraya que dichos Estados miembros tienen que respetar plenamente los intereses de la UE en su conjunto;

109. Considera que dichos acuerdos no deben vulnerar los tratados europeos, especialmente el principio de cooperación sincera (según el apartado 3 del artículo 4 del Tratado de la Unión Europea), ni socavar las políticas de la UE en general y, más específicamente, el mercado interior, la libre competencia ni el desarrollo económico, industrial y social; se reserva el derecho de activar los procedimientos del tratado en caso de que se demuestre que dichos acuerdos contradicen la cohesión de la Unión o los principios fundamentales sobre los que se basa;

Aspectos internacionales

110. Hace un llamamiento a la Comisión para que presente antes de enero de 2015 una estrategia de gobierno democrática de Internet;

111. Solicita a los Estados miembros que respondan al llamamiento de la 35ª Conferencia Internacional de Comisarios de Protección de Datos y de la Intimidad «para que aboguen por la adopción de un protocolo adicional del artículo 17 del Pacto internacional de derechos civiles y políticos (ICCPR), que debe basarse en los estándares que se han desarrollado y adoptado por la Conferencia Internacional y las disposiciones del comentario general nº 16 del Pacto para crear estándares aplicables en todo el mundo de protección de datos y de la intimidad de acuerdo con la ley»; solicita a la Alta Representante y Vicepresidenta de la Comisión y al Servicio de Acción Exterior que adopten una posición más activa;

112. Hace un llamamiento a los Estados miembros para que desarrollen una estrategia sólida y coherente dentro de las Naciones Unidas, y que apoyen en especial la

resolución sobre «el derecho a la intimidad en la era digital», presentada por Brasil y Alemania, tal y como la adoptó la Tercera Comisión de la Asamblea General de las Naciones Unidas (Comité de Derechos Humanos) el 27 de noviembre de 2013;

Plan de prioridades: un* habeas corpus *digital europeo

113. Decide presentar a los ciudadanos, instituciones y Estados miembros de la UE las recomendaciones indicadas como un plan de prioridades para la próxima legislatura;

114. Decide presentar un *habeas corpus* digital europeo para la protección de la intimidad a partir de las siete acciones siguientes con un organismo protector del Parlamento Europeo:

Acción 1: adopción del paquete de protección de datos en 2014;

Acción 2: cerrar el acuerdo marco entre la UE y los Estados Unidos que garantice los mecanismos de compensación adecuados para los ciudadanos europeos en caso de que se produzcan envíos de datos de la UE a los Estados Unidos para fines policiales;

Acción 3: suspender el sistema de puerto seguro hasta que se haya efectuado un análisis completo y se hayan enmendado las lagunas actuales para garantizar que el envío de datos personales con fines comerciales desde la Unión a los Estados Unidos solo pueda tener lugar de conformidad con los máximos estándares de la UE;

Acción 4: suspender el acuerdo TFTP hasta que i) se hayan cerrado las negociaciones del acuerdo general; ii) se haya efectuado una investigación exhaustiva a partir de un análisis de la UE y todos los problemas detectados por el Parlamento en su Resolución de 23 de octubre hayan sido debidamente abordados;

Acción 5: proteger la legalidad y los derechos fundamentales de los ciudadanos de la EU, con una atención especial a las amenazas a la libertad de prensa y el secreto profesional (incluidas las relaciones entre abogados y clientes) y a la mejora de la protección de los denunciantes de irregularidades;

Acción 6: desarrollar una estrategia europea de independencia de las tecnologías de la información (a nivel nacional y comunitario);

Acción 7: promover la UE como un actor de referencia en la gobernanza democrático y neutral de Internet;

115. Hace un llamamiento a las instituciones y Estados miembros de la UE para que respalden y promuevan el *habeas corpus* digital europeo; se compromete a actuar como el guardián de los derechos de los ciudadanos de la UE con el siguiente plan de seguimiento de la puesta en práctica:

- Abril-julio de 2014: grupo de seguimiento basado en el equipo de investigación

de la Comisión LIBE responsable del seguimiento de cualquier revelación nueva en los medios de comunicación en relación con el mandato de la investigación y de estudiar la puesta en práctica de esta resolución;

- Desde julio de 2014: un mecanismo permanente de control de intercambio de datos y recursos judiciales dentro de la comisión competente;

- Primavera de 2014: una petición formal al Consejo Europeo para que incluya el *habeas corpus* digital europeo en las directrices que deben adoptarse según el artículo 68 del TFUE;

- Otoño 2014: un compromiso de que el *habeas corpus* digital europeo y las recomendaciones relacionadas serán criterios fundamentales para la aprobación de la siguiente Comisión;

- 2014-2015: un grupo de derechos de los ciudadanos/datos/confianza que deberá reunirse periódicamente entre el Parlamento Europeo y el Congreso de los Estados Unidos, así como con los parlamentos de terceros países comprometidos, incluido Brasil;

- 2014-2015: una conferencia con los organismos de control de los servicios de inteligencia de los parlamentos nacionales europeos;

- 2015: una conferencia que reúna a expertos europeos del máximo nivel en los diversos ámbitos de la seguridad informática (como matemáticas, criptografía y tecnologías de mejora de la intimidad) para ayudar a fomentar una estrategia informática de la UE para la próxima legislatura;

116. Encarga a su Presidente que transmita la presente Resolución al Consejo Europeo, al Consejo, a la Comisión, a los Gobiernos y los Parlamentos de los Estados miembros, a las autoridades nacionales de protección de datos, a la SEPD, a eu-LISA, a ENISA, a la Agencia de Derechos Fundamentales, al Grupo de Trabajo del Artículo 29, al Consejo de Europa, al Congreso de los Estados Unidos de América, al Gobierno de los EE.UU., a la Presidenta, el Gobierno y el Parlamento de la República Federal de Brasil y al Secretario General de las Naciones Unidas.

EXPOSICIÓN DE MOTIVOS

«La misión del soberano, sea un monarca o una asamblea, consiste en el fin para el cual fue investido con el soberano poder, que no es otro sino procurar la seguridad del pueblo»
Hobbes, Leviatán (capítulo XXX)

«No podemos encomendar nuestra sociedad a otros apartándonos de los estándares fundamentales que la hacen digna de encomendar»
Lord Bingham de Cornhill,
Expresidente del Tribunal Supremo de Inglaterra y Gales

Metodología

A partir de julio de 2013, la Comisión de Investigación LIBE fue responsable de la dificilísima tarea de cumplir con el mandato[1] del plenario sobre la investigación de la vigilancia electrónica masiva de los ciudadanos de la UE en un plazo muy corto de menos de 6 meses.

Durante dicho periodo, mantuvo más de 15 vistas sobre cada uno de los conjuntos específicos de cuestiones indicados en la resolución de 4 de julio y empleó informes de expertos tanto europeos como estadounidenses que aúnan un amplio espectro de experiencia y conocimientos: instituciones de la UE, parlamentos nacionales, Congreso de EE.UU., académicos, periodistas, sociedad civil, especialistas en seguridad y tecnología y empresas privadas. Además, una delegación de la Comisión LIBE visitó Washington entre el 28 y el 30 de octubre de 2013 para reunirse con representantes de los poderes ejecutivo y legislativo (académicos, abogados, expertos en seguridad y representantes de empresas)[2]. A dicha ciudad también acudió al mismo tiempo una Comisión de Asuntos Exteriores (AFET). Varias reuniones se celebraron conjuntamente.

Varios documentos de trabajo[3] han sido corredactados por el ponente, los ponentes alternativos[4] de los diversos grupos políticos y 3 miembros de la Comisión de AFET[5] , para presentar los principales hallazgos de la investigación. El ponente desea agradecer a todos los ponentes alternativos y a los miembros de AFET por su estrecha colaboración y compromiso de alto nivel a lo largo de este exigente proceso.

[1] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_ta-prov(2013)0322_en.pdf
[2] Véase el informe de la delegación de Washington.
[3] Véase el anexo I.
[4] Lista de ponentes alternativos: Axel Voss (PPE), Sophia in't Veld (ALDE), Jan Philipp Albrecht (VERDES/ALE), Timothy Kirkhope (ELD), Cornelia Ernst (GUE).
[5] Lista de miembros de AFET: José Ignacio Salafranca Sánchez-Neyra (PPE), Ana Gomes (S&D), Annemie Neyts-Uyttebroeck (ALDE).

Magnitud del problema

El creciente protagonismo de la seguridad junto con los desarrollos tecnológicos han permitido que los Estados conozcan más datos que nunca sobre sus ciudadanos. Puesto que los servicios de inteligencia pueden recopilar datos relacionados con el contenido de las comunicaciones, así como metadatos, y supervisar las actividades electrónicas de los ciudadanos, en particular su utilización de teléfonos inteligentes y tabletas, pueden saber, de hecho, casi todo sobre una persona. Esto ha contribuido a un cambio fundamental en el trabajo y las prácticas de las agencias de inteligencia, que se aleja del concepto tradicional de vigilancia específica como una medida necesaria y proporcional contra el terrorismo y se encamina hacia sistemas de vigilancia masiva.

Este aumento de la vigilancia masiva no ha sido objeto de ningún debate público previo ni de ninguna toma de decisiones democrática. Hay que debatir la finalidad y el alcance de la vigilancia y qué lugar ocupa en una sociedad democrática. ¿Acaso constituye la situación creada por las revelaciones de Edward Snowden un indicio de un giro social en bloque hacia la aceptación del fin de la intimidad a cambio de seguridad? ¿Nos enfrentamos a violación de la intimidad de tal magnitud que no sólo los criminales, sino las empresas de telecomunicaciones y las agencias de inteligencia saben todos los detalles de la vida de los ciudadanos? ¿Se trata de un hecho que tenemos que aceptar sin más discusión? ¿O es responsabilidad del legislador adaptar las políticas y las herramientas legales a su disposición para limitar los riesgos y evitar mayores perjuicios en caso de que fuerzas menos democráticas accediesen al poder?

Reacciones a la vigilancia masiva y debate público

El debate sobre la vigilancia masiva no tiene lugar de forma uniforme dentro de la UE. De hecho, en muchos Estados miembros apenas hay debate público y la atención de los medios de comunicación varía. Parece que Alemania es el país donde las reacciones a las revelaciones han sido más enérgicas y el debate público sobre sus consecuencias ha sido generalizado. En el Reino Unido y Francia, a pesar de las investigaciones de *The Guardian* y *Le Monde*, las reacciones han sido más limitadas, un hecho que se ha vinculado a la supuesta implicación de sus servicios de inteligencia en actividades con la NSA. La investigación de la Comisión LIBE ha podido escuchar valiosas contribuciones de los organismos parlamentarios de control de Bélgica, los Países Bajos, Dinamarca e incluso Noruega; sin embargo, los parlamentos británico y francés han rechazado la participación. Estas diferencias muestran de nuevo la falta de uniformidad de los mecanismos de control y equilibrio dentro de la UE en estas cuestiones y que se necesita más cooperación entre los organismos parlamentarios a cargo de las tareas de control;

A partir de las revelaciones de Edward Snowden en los medios de comunicación, el debate público se ha basado a grandes rasgos en dos tipos de reacciones. Por una parte, hay quienes rechazan la legitimidad de la información publicada por considerar que la mayor parte de los informes de los medios se basan en interpretaciones erróneas; además, muchos, aunque no desmienten las revelaciones, argumentan que no son válidas debido a los supuestos riesgos

para la seguridad nacional y la lucha contra el terrorismo que acarrean.

Por otra parte, hay quienes consideran que la información facilitada precisa de un debate público e informado a causa de la magnitud de los problemas que plantea en cuestiones fundamentales para la democracia, como: el Estado de derecho, los derechos fundamentales, la intimidad de los ciudadanos, la rendición de cuentas pública de los servicios policiales y de inteligencia, etc. Así es sin duda para los periodistas y editores de los mayores medios de prensa del mundo que están al tanto de las revelaciones, como *The Guardian*, *Le Monde*, *Der Spiegel*, *The Washington Post* y Glenn Greenwald.

Los dos tipos de reacciones que se perfilan se basan en un conjunto de motivos que pueden conllevar decisiones contrapuestas sobre cómo debe reaccionar o no la UE.

5 razones para no actuar

– *El postulado de la seguridad nacional y la inteligencia: no incide en al ámbito de competencias de la UE.*

Las revelaciones de Edward Snowden están relacionadas con las actividades de los servicios de inteligencia de Estados Unidos y de algunos de los Estados miembros, pero la seguridad nacional es una competencia nacional, por lo que la UE no tiene competencias en dichos asuntos (excepto en la seguridad interna de la UE) y no es posible emprender acciones a nivel comunitario.

– *El postulado del terrorismo: el peligro de los denunciantes de irregularidades.*

Cualquier seguimiento de estas revelaciones, o su mera consideración, debilita aún más la seguridad de Estados Unidos y de la UE, ya que no condena la publicación de documentos cuyo contenido, incluso redactado tal y como explican los medios de comunicación, puede poner una valiosa información en manos de grupos terroristas.

– *El postulado de la traición: los denunciantes de irregularidades no tienen legitimidad*

Como algunos han propuesto, principalmente en Estados Unidos y Reino Unido, cualquier debate iniciado o acción prevista a partir de las revelaciones de Edward Snowden son intrínsecamente sesgados e irrelevantes, ya que se basan en un acto inicial de traición.

– *El postulado del realismo: intereses estratégicos generales*

Aunque se confirmasen errores y actividades ilegales, deben ponderarse frente a la necesidad de mantener las relaciones especiales entre Estados Unidos y Europa para conservar los intereses económicos, comerciales y de asuntos exteriores comunes.

– *El postulado del buen gobierno: hay que confiar en el Gobierno*

Los gobiernos de Estados Unidos y de la UE se eligen de forma democrática. En el ámbito de la seguridad, e incluso cuando las actividades de los servicios de inteligencia se llevan a cabo para luchar contra el terrorismo, cumplen con los estándares democráticos por principio. Esta «presunción de buen gobierno» se fundamenta no sólo en la buena

voluntad de los titulares de los poderes ejecutivos de estos Estados, sino también en el mecanismo de control y contrapeso consagrado en sus sistemas constitucionales.

Como se ve, hay muchas y sólidas razones para no actuar. Ésta puede ser la explicación de por qué muchos gobiernos de la UE, tras unas enérgicas reacciones iniciales, han optado por no actuar. La principal acción del Consejo de Ministros ha sido establecer un «grupo transatlántico de expertos en protección de datos» que se ha reunido en tres ocasiones y ha elaborado un informe final. Se supone que un segundo grupo se ha reunido para tratar temas relacionados con la inteligencia entre las autoridades de Estados Unidos y de los Estados miembros, pero no hay información disponible. El Consejo Europeo ha abordado el problema de la vigilancia en una simple declaración de Jefes de Estado o de Gobierno[1]. Hasta ahora, sólo algunos parlamentos nacionales han iniciado investigaciones.

5 razones para actuar

– *El postulado de la vigilancia masiva: ¿en qué sociedad queremos vivir?*

A partir de la primera revelación en junio de 2013, ha habido constantes referencias a la novela «1984» de George Orwell. Desde los ataques del 11 de septiembre de 2001, el protagonismo de la seguridad y el cambio hacia una vigilancia específica ha dañado y socavado el concepto de la intimidad. La Historia, tanto de Europa como de Estados Unidos, muestra los peligros de la vigilancia masiva y la degradación hacia las sociedades sin intimidad.

– *El postulado de los derechos fundamentales:*

La vigilancia masiva e indiscriminada amenaza los derechos fundamentales de los ciudadanos, como el derecho a la intimidad, la protección de datos, la libertad de prensa o un juicio justo, todos ellos consagrados en los tratados de la UE, la Carta de los Derechos Fundamentales y el CEDH. Estos derechos no pueden burlarse ni negociarse por posibles ventajas a cambio a menos que así esté dispuesto en instrumentos legales y de conformidad con los tratados.

– El postulado de la seguridad interna de la UE:

Las competencias nacionales en cuestiones de inteligencia y seguridad nacional no excluyen una competencia paralela de la UE. La UE ha ejercido las competencias concedidas por los Tratados de la UE en cuestiones de seguridad interna decidiendo sobre varios instrumentos legislativos y acuerdos internacionales con el objetivo de luchar contra el crimen y el terrorismo y sobre el establecimiento de una estrategia interna y agencias de seguridad para trabajar en este ámbito. Además, se han desarrollado otros servicios que reflejan la necesidad de una mayor cooperación a nivel comunitario en

[1] Conclusiones del Consejo Europeo del 24-25 de octubre de 2013, en especial: «Los Jefes de Estado o de Gobierno han tomado nota de la intención de Francia y Alemania de tratar de organizar conversaciones bilaterales con los EE.UU. a fin de alcanzar antes de finales de año un entendimiento sobre las relaciones mutuas en ese ámbito. Han tomado nota de que los demás países de la UE que deseen sumarse a esta iniciativa serán bienvenidos. Asimismo, se han referido al grupo de trabajo existente entre la UE y los EE.UU. sobre la cuestión conexa de la protección de datos y han pedido que se avance con rapidez y con ánimo constructivo al respecto».

cuestiones relacionadas con la inteligencia: INTCEN (dentro del EEAS) y el Coordinador Antiterrorista (dentro de la Secretaría General del Consejo), ninguno de los cuales cuenta con base legal.

– *El postulado del control deficiente:*

Aunque los servicios de inteligencia llevan a cabo una función indispensable en la protección frente a las amenazas internas y externas, tienen que actuar dentro de los límites del Estado de derecho, y, para ello, tienen que estar sometidos a un estricto y exhaustivo mecanismo de control. El control democrático de las actividades de los servicios de inteligencia se lleva a cabo a nivel nacional, pero debido a la naturaleza internacional de los peligros para la seguridad, actualmente hay un gran intercambio de información entre los Estados miembros y con terceros países como Estados Unidos; se necesita realizar mejoras en los mecanismos de control tanto a nivel nacional como comunitario si no se quiere que los mecanismos tradicionales de control queden ineficaces y desfasados.

– *El efecto negativo sobre los medios de comunicación y la protección de los denunciantes de irregularidades*

Las revelaciones de Edward Snowden y las posteriores publicaciones en los medios de comunicación han destacado el papel crucial de la prensa en una democracia para garantizar la rendición de cuentas de los gobiernos. Cuando los mecanismos de supervisión no evitan ni corrigen la vigilancia masiva, es muy importante el papel de los medios de comunicación y los denunciantes de irregularidades al desvelar posibles ilegalidades o abusos de poder. Las reacciones de las autoridades de Estados Unidos y Reino Unido contra los medios han demostrado la vulnerabilidad tanto de la prensa como de los denunciantes y la urgente necesidad de emprender más acciones para protegerlos.

La Unión Europea tiene que elegir entre una política de *statu quo* (hay suficientes razones para no actuar, esperar y ver) y una política de evaluación de la realidad (la vigilancia no es nueva, pero hay pruebas suficientes de una escala sin precedentes en el alcance y la capacidad de las agencias de inteligencia que hacen preciso que la UE actúe).

El *habeas corpus* en una sociedad vigilada

En 1679, el Parlamento Británico adoptó la Ley de *habeas corpus* como un gran avance para garantizar el derecho a un juez en tiempos de jurisdicciones rivales y conflictos de leyes. Actualmente, nuestras democracias garantizan derechos suficientes a los condenados o detenidos que sean objeto de un proceso penal o hayan sido remitidos a un tribunal. Sin embargo, sus datos, tal y como se han registrado, procesado, almacenado y mantenido en redes digitales conforman un «cuerpo de datos personales», una especie de cuerpo digital específico para cada persona y que puede revelar gran parte de su identidad, hábitos y preferencias.

El *habeas corpus* está reconocido como un instrumento legal fundamental para salvaguardar

las libertades individuales frente a la acción arbitraria del Estado. Lo que se necesita actualmente es una ampliación del *habeas corpus* para la era digital. El derecho a la intimidad, el respeto de la integridad y la dignidad de las personas están en juego. La recogida masiva de datos sin respetar las normas de protección de datos de la UE y la vulneración específica del principio de proporcionalidad en la gestión de datos son contrarias a las tradiciones constitucionales de los Estados miembros y a los fundamentos del orden constitucional europeo.

La principal novedad actualmente es que estos riesgos no sólo están originados en actividades criminales (frente a las cuales los legisladores de la UE han adoptado una serie de instrumentos) o en posibles ciberataques de gobiernos con un pobre historial democrático. Se ha hecho evidente que dichos riesgos también pueden tener su origen en los servicios policiales o de inteligencia de países democráticos, lo que conlleva que los ciudadanos y empresas de la UE se ven envueltos en conflictos de leyes e incertidumbres legales, con posibles vulneraciones de sus derechos y sin mecanismos de compensación adecuados.

El gobierno de las redes es necesario para garantizar la seguridad de los datos personales. Antes de que los Estados modernos se desarrollasen, no se podía garantizar la seguridad en las carreteras ni en las calles de las ciudades, y la integridad física estaba en peligro. Actualmente, a pesar de que dominan la vida diaria, las autopistas de la información no son seguras. Se ha de proteger la integridad de los datos digitales no sólo frente a los criminales, sino también frente a los posibles abusos de poder por parte de las autoridades de los Estados o contratistas y empresas privadas con garantías judiciales secretas.

Recomendaciones de la investigación de la Comisión LIBE

Muchos de los problemas planteados hoy en día son muy parecidos a los revelados por la investigación del Parlamento Europeo sobre el programa Echelon en 2001. La imposibilidad de realizar un seguimiento de los hallazgos y recomendaciones de la Comisión Echelon en la legislatura anterior debería servir de lección a la investigación actual. Es por ello que esta resolución, que reconoce tanto la magnitud de las revelaciones como su naturaleza continuada, permite planificar a largo plazo y garantiza que hay propuestas específicas en la mesa para las acciones de seguimiento en la siguiente legislatura parlamentaria que garanticen que los resultados sigan en la orden del día de la agenda política de la UE.

A partir de esta evaluación, el ponente desea someter a votación parlamentaria las siguientes cuestiones:

Un *habeas corpus* digital europeo para la protección de la intimidad basado en 7 acciones:

Acción 1: adopción del paquete de protección de datos en 2014;

Acción 2: cerrar el acuerdo general entre la UE y Estados Unidos que garantice los mecanismos de compensación adecuados para los ciudadanos europeos en caso de que se produzcan envíos de datos de la UE a Estados Unidos para fines policiales;

Acción 3: suspender el sistema de puerto seguro hasta que se haya efectuado un análisis completo y se hayan enmendado las lagunas actuales para garantizar que el

envío de datos personales con fines comerciales desde la Unión a Estados Unidos sólo pueda tener lugar de conformidad con los máximos estándares de la UE;

Acción 4: suspender el acuerdo TFTP hasta que i) se hayan cerrado las negociaciones del acuerdo general; ii) se haya efectuado una investigación exhaustiva a partir de un análisis de la UE y todas los problemas detectados por el Parlamento en su resolución de 23 de octubre hayan sido debidamente abordados;

Acción 5: proteger la legalidad y los derechos fundamentales de los ciudadanos de la EU, con una atención especial a las amenazas a la libertad de prensa y el secreto profesional (incluidas las relaciones entre abogados y clientes) y a la mejora de la protección de los denunciantes de irregularidades;

Acción 6: desarrollar una estrategia europea de independencia de las tecnologías de la información (a nivel nacional y comunitario);

Acción 7: promover la UE como un actor de referencia en el gobierno democrático y neutral de Internet;

Tras la conclusión de la investigación, el Parlamento Europeo debe seguir actuando como protector de los derechos de los ciudadanos de la UE con el siguiente programa para hacer un seguimiento de las implementaciones:

- Abril-julio de 2014: grupo de seguimiento basado en el equipo de investigación de la Comisión LIBE responsable del seguimiento de cualquier revelación nueva en los medios de comunicación en relación con el mandato de la investigación y de estudiar la puesta en práctica de esta resolución;

- Desde julio de 2014: un mecanismo permanente de control de intercambio de datos y recursos judiciales dentro de la comisión competente;

- Primavera de 2014: una petición formal al Consejo Europeo para que incluya el *habeas corpus* digital europeo en las directrices que deben adoptarse según el artículo 68 del TFUE;

- Otoño 2014: un compromiso de que el *habeas corpus* digital europeo y las recomendaciones relacionadas serán criterios fundamentales para la aprobación de la siguiente Comisión;

- 2014-2015: un grupo de derechos de los ciudadanos/datos/confianza deberá reunirse periódicamente entre el Parlamento Europeo y el Congreso de Estados Unidos, así como con los parlamentos de terceros países comprometidos, incluido Brasil;

- 2014-2015: una conferencia con los organismos de control de los servicios de inteligencia de los parlamentos nacionales europeos;

- 2015: una conferencia que reúna a expertos europeos del máximo nivel en los diversos ámbitos de la seguridad informática (como matemáticas, criptografía y tecnologías de mejora de la intimidad) para ayudar a fomentar una estrategia informática de la UE para la próxima legislatura;

ANEXO I: LISTA DE DOCUMENTOS DE TRABAJO

Investigación de la Comisión LIBE

Ponente de opinión y ponentes alternativos como coautores	Temas	Resolución del PE de 4 de julio de 2013 (véanse los apartados 15-16)
Sr. Moraes (S&D)	Programas de vigilancia de los Estados Unidos y los Estados miembros de la UE y su repercusión sobre los derechos fundamentales de los ciudadanos europeos	16 (a) (b) (c) (d)
Sr. Voss (PPE)	**Actividades de vigilancia de los Estados Unidos con respecto a los datos de la UE y sus posibles consecuencias legales para los acuerdos y la cooperación transatlánticos**	16 (a) (b) (c)
Sra. In't Veld (ALDE) y Sr. Ernst (GUE)	Supervisión democrática de los servicios de inteligencia de los Estados miembros y de los organismos de inteligencia de la UE	15, 16 (a) (c) (e)
Sr. Albrecht (VERDES/ALE)	Relación entre las prácticas de vigilancia de la UE y los EE.UU. y las disposiciones de protección de datos de la UE	16 (c) (e) (f)
Sr. Kirkhope (CRE)	Alcance de la seguridad internacional, europea y nacional en la perspectiva de la UE	16 (a) (b)
3 miembros de AFET	Aspectos de política exterior de la investigación sobre la vigilancia electrónica masiva de los ciudadanos de la UE	16 (a) (b) (f)

ANEXO II: LISTA DE VISTAS Y EXPERTOS

INVESTIGACIÓN DE LA COMISIÓN LIBE
SOBRE EL PROGRAMA DE VIGILANCIA DE LA NSA ESTADOUNIDENSE
Y DE ORGANISMOS DE VIGILANCIA EN VARIOS ESTADOS MIEMBROS
Y SUS REPERCUSIONES EN LOS DERECHOS FUNDAMENTALES DE LOS
CIUDADANOS DE LA UE Y EN LA COOPERACIÓN TRANSATLÁNTICA EN
ASUNTOS DE JUSTICIA E INTERIOR

A partir de la resolución del Parlamento Europeo del 4 de julio de 2013 (apartado 16), la Comisión LIBE ha realizado una serie de vistas para reunir información en relación con los distintos aspectos que hay tener en cuenta, evaluar las repercusiones de las actividades de vigilancia en cuestión, especialmente en lo que concierne a derechos fundamentales y normas de protección de datos, considerar mecanismos de compensación y proponer recomendaciones para proteger los derechos de los ciudadanos de la UE y fortalecer la seguridad informática de las instituciones comunitarias.

Fecha	Asunto	Expertos
5 de septiembre de 2013, 15.00 – 18.30 (BXL)	- Intercambio de opiniones con los periodistas que habían revelado el caso y publicado los hechos	• Jacques FOLLOROU, *Le Monde* • Jacob APPELBAUM, periodista de investigación, desarrollador de software e investigador de seguridad informática en el proyecto Tor • Alan RUSBRIDGER, jefe de redacción de Guardian News and Media (por videoconferencia)
	- Seguimiento de la comisión temporal sobre el sistema de interceptación ECHELON	• Carlos COELHO (parlamentario europeo), expresidente de la comisión temporal sobre el sistema de interceptación ECHELON • Gerhard SCHMID

		(exparlamentario europeo y ponente el informe ECHELON 2001) • Duncan CAMPBELL, periodista de investigación y autor del informe STOA «Capacidad de interceptación 2000»
12 de septiembre de 2013, 10.00 – 12.00 (STR)	- Comentarios sobre la reunión del grupo de expertos transatlántico UE-EE.UU. sobre la protección de datos del 19/20 de septiembre de 2013. Método de trabajo y cooperación con la investigación de la Comisión LIBE (en vídeo) - Intercambio de opiniones con el grupo de trabajo sobre protección de datos Artículo 29	• Darius ŽILYS, Presidencia del Consejo, director del departamento de Derecho internacional, Ministerio de Justicia de Lituania (copresidente del grupo de trabajo UE-EE.UU. *ad hoc* sobre protección de datos) • Paul NEMITZ, director de la Dirección General de Justicia de la Comisión Europea (copresidente del grupo de trabajo UE-EE.UU. *ad hoc* sobre protección de datos) • Reinhard PRIEBE, director de la Dirección General de Interior de la Comisión Europea (copresidente del grupo de trabajo UE-EE.UU. *ad hoc* sobre protección de datos) • Jacob KOHNSTAMM, presidente
24 de septiembre de 2013, 9.00 – 11.30 y 15.00 – 18.30 (BXL) **Con AFET**	- Presunta interceptación de los datos SWIFT empleados en el programa TFTP por parte de la NSA - Comentarios sobre la reunión del	• Cecilia MALMSTRÖM, miembro de la Comisión Europea • Rob WAINWRIGHT, director de Europol • Blanche PETRE, consejera general de SWIFT • Darius ŽILYS, Presidencia del

	grupo de expertos transatlántico UE-EE.UU. sobre la protección de datos del 19/20 de septiembre de 2013 - Intercambio de opiniones con la sociedad civil estadounidense (parte I) - Eficacia de la vigilancia en la lucha contra el crimen y el terrorismo en Europa - Presentación del estudio sobre los programas de vigilancia de Estados Unidos y sus repercusiones en la intimidad de los ciudadanos de la UE	Consejo, director del departamento de Derecho internacional, Ministerio de Justicia de Lituania (copresidente del grupo de trabajo UE-EE.UU. *ad hoc* sobre protección de datos) • Paul NEMITZ, director de la Dirección General de Justicia de la Comisión Europea (copresidente del grupo de trabajo UE-EE.UU. *ad hoc* sobre protección de datos) • Reinhard PRIEBE, director de la Dirección General de Interior de la Comisión Europea (copresidente del grupo de trabajo UE-EE.UU. *ad hoc* sobre protección de datos) • Jens-Henrik JEPPESEN, director de asuntos europeos del Center for Democracy & Technology (CDT) • Greg NOJEIM, consejero principal y director del proyecto sobre libertad, seguridad y tecnología del Center for Democracy & Technology (CDT) (por videoconferencia) • Dr. Reinhard KREISSL, coordinador de Increasing Resilience in Surveillance Societies (IRISS) (por videoconferencia) • Caspar BOWDEN, investigador independiente, exasesor principal sobre privacidad de Microsoft, autor de la nota del departamento de políticas encargada por la

		Comisión LIBE sobre los programas de vigilancia de Estados Unidos y sus repercusiones en la intimidad de los ciudadanos de la UE
30 de septiembre de 2013, 15.00 – 18.30 (BXL) **Con AFET**	- Intercambio de opiniones con la sociedad civil estadounidense (parte II) - Actividades de los denunciantes de irregularidades en el ámbito de la vigilancia y su protección legal	• Marc ROTENBERG, Electronic Privacy Information Centre (EPIC) • Catherine CRUMP, Unión Estadounidense por las Libertades Civiles (ACLU) Declaraciones de denunciantes: • Thomas DRAKE, exresponsable de la NSA • J. Kirk WIEBE, exanalista principal de la NSA • Annie MACHON, exfuncionaria de inteligencia del MI5 Declaraciones de ONG sobre la protección legal de los denunciantes: • Jesselyn RADACK, abogada y representante de 6 denunciantes, Government Accountability Project • John DEVITT, Transparencia Internacional Irlanda
3 de octubre de 2013, 16.00 - 18.30 (BXL)	- Supuesta piratería o intercepción de los sistemas de Belgacom por parte de los servicios de inteligencia (GCHQ británico)	• Geert STANDAERT, vicepresidente del motor de prestación de servicios, BELGACOM S.A. • Dirk LYBAERT, secretario general, BELGACOM S.A. • Frank ROBBEN, Commission de la Protection de la Vie Privée Belgique, coponente del «dosier Belgacom»
7 de octubre	- Repercusiones de los programas	• Imke SOMMER, Die

de 2013, 19.00 – 21.30 (STR)	de vigilancia estadounidenses sobre el puerto seguro de EE.UU. - Repercusiones de los programas de vigilancia estadounidenses sobre otros instrumentos de transferencia internacional (cláusulas contractuales, normas corporativas vinculantes)	Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (ALEMANIA) • Christopher CONNOLLY – Galexia • Peter HUSTINX, Autoridad europea para la protección de datos (AEPD) • **Isabelle FALQUE-PIERROTIN,** presidente de CNIL (FRANCIA)
14 de octubre de 2013, 15.00 – 18.30 (BXL)	- Vigilancia electrónica masiva de ciudadanos de la UE y legislación internacional, comunitaria y del Consejo de Europa - Casos judiciales sobre programas de vigilancia	• Martin SCHEININ, antiguo ponente especial de la ONU sobre el fomento y la protección de los derechos humanos en la lucha antiterrorista, profesor del Instituto Universitario Europeo y líder del proyecto FP7 «SURVEILLE» • Bostjan ZUPANČIČ, juez del TEDH (por videoconferencia) • Douwe KORFF, profesor de Derecho, Universidad Metropolitana de Londres • Dominique GUIBERT, vicepresidente de la Ligue des Droits de l'Homme (LDH) • Nick PICKLES, director de Big Brother Watch • Constanze KURZ, informática, jefa de proyectos del Forschungszentrum für Kultur

		und Informatik
7 de noviembre de 2013, 9.00 - 11.30 y 15.00 – 18.30 (BXL)	- El papel del IntCen de la UE en las actividades de inteligencia de la UE (por vídeo) - Programas nacionales de vigilancia masiva de los datos personales en los Estados miembros de la UE y su compatibilidad con la legislación comunitaria - El papel del control parlamentario de los servicios de inteligencia a nivel nacional en una era de vigilancia masiva (parte I) (Comisión de Venecia) (Reino Unido) - Grupo de expertos transatlántico UE-EE.UU.	• Ilkka SALMI, director del Centro de Análisis de Inteligencia de la UE (IntCen) • Sergio CARRERA, investigador principal y director de la sección de Justicia e Interior del Centro de Estudios Políticos Europeos (CEPS), Bruselas • Francesco RAGAZZI, catedrático adjunto en Relaciones Internacionales, de la Universidad de Leiden • Iain CAMERON, miembro de la Comisión Europea para la Democracia por el Derecho (Comisión de Venecia) • Ian LEIGH, catedrático de Derecho, Universidad de Durham • David BICKFORD, exdirector jurídico de las agencias de inteligencia MI5 y MI6 • Gus HOSEIN, director ejecutivo, Privacy International • Paul NEMITZ, Derechos fundamentales y ciudadanía, Dirección General de Justicia, Comisión Europea • Reinhard PRIEBE, Gestión de crisis y seguridad interna, Dirección General de Interior, Comisión Europea
11 de noviembre de 2013 15.00 - 18.30 (BXL)	- Programas de vigilancia estadounidenses y sus repercusiones sobre la intimidad de los ciudadanos de la UE (declaración de Jim	• Jim SENSENBRENNER, Cámara de Representantes de Estados Unidos (miembro del Comité de Asuntos Jurídicos y presidente del subcomité sobre

	SENSENBRENNER, diputado del Congreso de EE.UU.) - El papel del control parlamentario de los servicios de inteligencia a nivel nacional en una era de vigilancia masiva (NL,SW) (parte II) - Programas estadounidenses de la NSA para la vigilancia electrónica masiva y el papel de las empresas de telecomunicaciones (Microsoft, Google, Facebook)	crimen, terrorismo, seguridad nacional e investigaciones) • Peter ERIKSSON, presidente de la Comisión Constitucional, Parlamento de Suecia (Riksdag) • A.H. VAN DELDEN, presidente de la Comisión Holandesa de Evaluación Independiente de los Servicios Policiales y de Inteligencia (CTIVD) • Dorothee BELZ, vicepresidenta de asuntos jurídicos y corporativos para Europa, Oriente Medio y África • Mr Nicklas LUNDBLAD, director de políticas públicas y relaciones institucionales, Google • Richard ALLAN, director de políticas públicas para Europa, Oriente Medio y África, Facebook
14 de noviembre de 2013, 15.00 – 18.30 (BXL) **Con AFET**	- Seguridad informática de las instituciones de la UE (parte I) (PE, COM (CERT-EU), (eu-LISA)) - El papel del control parlamentario de los servicios de inteligencia a nivel nacional en una era de vigilancia masiva (parte III) (BE, DA)	• Mr Giancarlo VILELLA, director general de innovación y asistencia tecnológica del Parlamento Europeo • Mr Ronald PRINS, director y cofundador de Fox-IT • Mr Freddy DEZEURE, responsable del grupo operativo CERT-EU, Dirección General de Informática de la Comisión Europea • Luca ZAMPAGLIONE, funcionario de seguridad, eu-LISA • Armand DE DECKER,

		vicepresidente del Senado de Bélgica, miembro de la Comisión de Seguimiento de la Comisión de Control de los Servicios de Inteligencia • Guy RAPAILLE, presidente de la Comisión de Control de los Servicios de Inteligencia (Comité R) • Karsten LAURITZEN, miembro de la Comisión de Asuntos Jurídicos, portavoz de asuntos jurídicos, Parlamento de Dinamarca
18 de noviembre de 2013, 19.00 – 21.30 (STR)	- Casos judiciales y otras denuncias de los programas de vigilancia nacionales (parte II) (ONG polaca)	• Adam BODNAR, vicepresidente de la junta, Fundación Helsinki para los Derechos Humanos (Polonia)
2 de diciembre de 2013, 15.00 – 18.30 (BXL)	- El papel del control parlamentario de los servicios de inteligencia a nivel nacional en una era de vigilancia masiva (parte IV) (Noruega)	• Michael TETZSCHNER, miembro del Comité Permanente de Control Público y Asuntos Constitucionales, Noruega (Stortinget)
5 de diciembre de 2013, 15.00 – 18.30 (BXL)	- Seguridad informática de las instituciones de la UE (parte II) - Repercusiones de la vigilancia masiva en la confidencialidad de las relaciones entre abogados y clientes	• Olivier BURGERSDIJK, responsable de estrategia, Centro Europeo de Ciberdelincuencia, EUROPOL • Udo HELMBRECHT, director ejecutivo de ENISA • Florian WALTHER, asesor de seguridad informática independiente • Jonathan GOLDSMITH, secretario general, Consejo de la Abogacía Europea (CCBE)
9 de diciembre de 2013 (STR)	- Recuperación de la confianza en los flujos de datos entre la UE y EE.UU.	• Viviane REDING, vicepresidenta de la Comisión Europea • Arcadio DÍAZ TEJERA,

	- Resolución 1954 del Consejo de Europa (2013) sobre «seguridad nacional y acceso a la información»	miembro del Senado de España, miembro de la Asamblea Parlamentaria del Consejo de Europa y ponente de su resolución 1954 (2013) sobre «seguridad nacional y acceso a la información»
17-18 de diciembre (BXL)	Comisión Parlamentaria de Investigación sobre el Espionaje al Senado de Brasil (videoconferencia) Medios informáticos de protección de la intimidad Intercambio de opiniones con el periodista que publicó los hechos (parte II) (videoconferencia)	• Vanessa GRAZZIOTIN, presidenta de la Comisión Parlamentaria de Investigación sobre el Espionaje • Ricardo DE REZENDE FERRAÇO, ponente de la Comisión Parlamentaria de Investigación sobre el Espionaje • Bart PRENEEL, catedrático de seguridad informática y criptografía industrial en la Universidad Católica de Lovaina, Bélgica • Stephan LECHNER, director del Instituto de Protección y Seguridad del Ciudadano (IPSC), Centro Común de Investigación (CCI), Comisión Europea • Christopher SOGHOIAN, tecnólogo principal, proyecto de libre expresión, intimidad y tecnología, Unión Estadounidense por las Libertades Civiles • Christian HORCHERT, asesor de seguridad informática, Alemania • Glenn GREENWALD, escritor y columnista centrado en la seguridad nacional y las libertades civiles, previamente en *The Guardian*

ANEXO III: LISTA DE EXPERTOS QUE RECHAZARON PARTICIPAR EN LAS VISTAS PÚBLICAS DE LA INVESTIGACIÓN LIBE

1. Expertos que rechazaron la invitación del presidente de LIBE

Estados Unidos

- Keith Alexander, general del Ejército de Estados Unidos, director de la NSA[1]
- Robert S. Litt, consejero general, Oficina del Director de Inteligencia Nacional[2]
- Robert A. Wood, encargado de negocios, representante de Estados Unidos ante la Unión Europea

Reino Unido

- Sir Iain Lobban, director del Cuartel General de Comunicaciones del Gobierno del Reino Unido (GCHQ)

Francia

- M. Bajolet, DirecTUEr général de la Sécurité Extérieure, Francia
- M. Calvar, DirecTUEr Central de la Sécurité Intérieure, Francia

Países Bajos

- Ronald Plasterk, ministro del Interior y de las Relaciones del Reino de los Países Bajos
- Ivo Opstelten, ministro de Seguridad y Justicia de los Países Bajos

Polonia

- Dariusz Łuczak, responsable de la Agencia de Seguridad Interior de Polonia
- Maciej Hunia, responsable de la Agencia de Inteligencia Exterior de Polonia

Empresas privadas de tecnologías de la información

[1] El ponente se entrevistó con Keith Alexander junto con el presidente Brok y el senador Feinstein en Washington el 29 de octubre de 2013.
[2] La delegación LIBE se reunió con Robert S. Litt en Washington el 29 de octubre de 2013.

- Tekedra N. Mawakana, responsable mundial de políticas públicas y viceconsejero general, Yahoo
- Saskia Horsch, directivo de políticas públicas, Amazon

Empresas de telecomunicaciones de la UE

- La Sra. Doutriaux, Orange
- Larry Stone, presidente de asuntos públicos e institucionales del grupo, British Telecom, Reino Unido
- Telekom, Alemania
- Vodafone

2. Expertos que no respondieron a la invitación del presidente de LIBE

Alemania

- Gerhard Schindler, Präsident des Bundesnachrichtendienstes

Países Bajos

- La Sra. Berndsen-Jansen, Voorzitter Vaste Kamer Commissie voor Binnenlandse Zaken Tweede Kamer der Staten-Generaal, Nederland
- Rob Bertholee, DirecTUEr Algemene Inlichtingen en Veiligheidsdienst (AIVD)

Suecia

- Ingvar Åkesson, Centro Nacional de Radiotransmisiones con fines de Defensa (Försvarets radioanstalt, FRA)