

Programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., órganos de vigilancia en diversos Estados miembros e impacto en los derechos fundamentales de los ciudadanos

Resolución del Parlamento Europeo, de 12 de marzo de 2014, 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 141,
- 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 el 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 de Viena sobre relaciones diplomáticas y, en particular, sus artículos 24, 27 y 40,
- 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

¹ <http://www.un.org/en/documents/udhr/>

terrorismo, presentado el 17 de mayo de 2010¹,

- Vista la Comunicación de la Comisión titulada «La política y la gobernanza de Internet – El papel de Europa en la configuración de la gobernanza de Internet» (COM(2014)0072);
- 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 2013²,
- 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 n° 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 2007³, 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 franceses⁴, polacos y británicos⁵, y ante el Tribunal Europeo de Derechos Humanos⁶, 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 III⁷,
- Vista la Decisión 2000/520/CE 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,

1 <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement>

2 http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

3 [http://www.venice.coe.int/webforms/documents/CDL-AD\(2007\)016.aspx](http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx)

4 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 Primera Instancia de París.

5 Casos de Privacy International y Liberty en el Tribunal de Poderes de Investigación.

6 Solicitud conjunta en virtud del artículo 34 de Big Brother Watch, Open Rights Group, English PEN y Dr. Constanze Kurz (demandantes) contra Reino Unido (demandado).

7 DO C 197 de 12.7.2000, p. 1.

- 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)0196) 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 de 2013, 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 estadounidenses de puerto seguro y preguntas más frecuentes relacionadas publicadas por el Departamento de Comercio de los EE.UU.¹, que consideraba que no podía confirmarse la adecuación del sistema, y los dictámenes del Grupo de Trabajo del Artículo 29, más concretamente el dictamen 4/2000, de 16 de mayo de 2000²,
- 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, 20073 y 20124,
- Vista la revisión conjunta de la aplicación del Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos⁵, que acompaña al Informe de la Comisión al Parlamento Europeo y al Consejo sobre la revisión conjunta (COM(2013)0844),
- Vistas las conclusiones del Abogado General Sr. Cruz Villalón, en las 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 Carta⁶,
- 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 la Comisión y del Consejo que la acompañan,
- Visto el Acuerdo de Asistencia Judicial entre la Unión Europea y los Estados Unidos de

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 11.8.2012, p. 5.

⁵ SEC(2013)0630 de 27.11.2013.

⁶ Conclusiones del Abogado General Sr. Cruz Villalón presentadas el 12 de diciembre de 2013 en el asunto C-293/12.

⁷ DO L 195 de 27.7.2010, p. 3.

América¹,

- 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) n° 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 derivadas de ella²,
- 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 n° 12333, emitido por el Presidente de los Estados Unidos en 1981 y modificado en 2008,
- Vista la Directiva Presidencial (Presidential Policy Directive, PPD-28) sobre actividades de inteligencia de señales, emitida por el Presidente de los EE.UU., Barack Obama, el 17 de enero de 2014,
- Vistas las propuestas legislativas que están siendo examinadas actualmente en el Congreso de los EE.UU., incluidos el proyecto de Ley sobre libertades de los EE.UU., el proyecto de Ley de reforma de la supervisión y vigilancia de inteligencia, y otros,
- 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 n° 13-0851 de 16 de diciembre de 2013, y la sentencia del tribunal de distrito del Distrito Sur de Nueva York de los Estados Unidos, ACLU et al. contra James R. Clapper et al., acción civil n° 13-3994 de 11 de junio de 2013,
- Visto el informe relativo a las conclusiones de los copresidentes de la UE del grupo de

¹ DO L 181 de 19.7.2003, p. 34.

² DO L 309 de 29.11.1996, p.1.

- trabajo *ad hoc* UE-EE.UU. sobre protección de datos, de 27 de noviembre de 20131,
- Vistas sus Resoluciones, de 5 de septiembre de 2001² y 7 de noviembre de 2002³, 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 UE⁴,
 - 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 UE⁵, por la cual encargó a su Comisión de Libertades Civiles, Justicia y Asuntos de Interior que llevara a cabo una investigación en profundidad de la cuestión,
 - Visto el documento de trabajo 1 sobre los programas de vigilancia de los Estados Unidos y la UE, y su repercusión sobre los derechos fundamentales de los ciudadanos europeos,
 - Visto el documento de trabajo 3 sobre la relación entre las prácticas de vigilancia de la UE y los EE. UU. y las disposiciones de protección de datos de la UE,
 - Visto el documento de trabajo 4 sobre las 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,
 - Visto el documento de trabajo 5 sobre la supervisión democrática de los servicios de inteligencia de los Estados miembros y de los organismos de inteligencia de la UE,
 - Visto el documento de trabajo de la Comisión de Asuntos Exteriores sobre los aspectos de política exterior de la investigación sobre la vigilancia electrónica masiva de los ciudadanos de la UE,
 - 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 cabo⁶,
 - Vista su Resolución, de 23 de octubre de 2013, sobre la suspensión del acuerdo TFTP a raíz de la vigilancia de la NSA⁷,
 - Vista su Resolución, de 10 de diciembre de 2013, sobre la liberación del potencial de la computación en la nube en Europa⁸,

¹ Documento 16987/2013 del Consejo.

² DO C 72 E de 21.3.2002, p. 221.

³ DO C 16 E de 22.1.2004, p. 88.

⁴ Textos Aprobados, P7_TA(2013)0203.

⁵ Textos Aprobados, P7_TA(2013)0322.

⁶ Textos Aprobados P7_TA(2013)0444.

⁷ Textos Aprobados P7_TA(2013)0449.

⁸ Textos Aprobados P7_TA(2013)0535.

- 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 común¹,
- 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 (A7-0139/2014),

El impacto de la vigilancia masiva

- A. Considerando que la protección de datos y la intimidad son derechos fundamentales; que las medidas de seguridad, incluidas las medidas de lucha contra el terrorismo, deben perseguirse a través del Estado de Derecho y deben estar sujetas a las obligaciones en materia de derechos fundamentales, incluidas las relacionadas con la intimidad y la protección de datos;
- B. Considerando que los datos y los flujos de información, que dominan actualmente la vida cotidiana y forman parte de la integridad de toda persona, deben estar tan protegidos de la intrusión como los hogares privados;
- C. Considerando que los lazos entre Europa y los Estados Unidos de América se basan en el espíritu y los principios de democracia, Estado de Derecho, libertad, justicia y solidaridad;
- D. Considerando que la cooperación en materia de lucha contra el terrorismo entre los Estados Unidos y la Unión Europea y sus Estados miembros sigue siendo vital para la seguridad de ambos socios;
- E. Considerando que la confianza y el entendimiento mutuos son factores claves en el diálogo y la asociación transatlánticos;
- F. Considerando que, a raíz del 11 de septiembre de 2001, la lucha contra el terrorismo se convirtió en una de las principales prioridades de la mayoría de los gobiernos; que las revelaciones basadas en los documentos filtrados por el excontratista de la Agencia Nacional de Seguridad Edward Snowden obligaron a los líderes políticos a abordar los retos de supervisar y controlar a las agencias de inteligencia en las actividades de vigilancia y a evaluar el impacto de sus actividades en los derechos fundamentales y el Estado de Derecho en una sociedad democrática;
- G. 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 Unidos como en los Estados miembros de la UE;

1 DO C 353 E de 3.12.2013, p. 156.

- a la violación de las normas jurídicas y en materia de derechos fundamentales y protección de datos de la UE;
 - al grado de confianza entre la UE y los EE.UU. en tanto que socios trasatlánticos;
 - 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;
 - a la falta 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 lucha contra el terrorismo en su sentido estricto, como por ejemplo, para el espionaje económico e industrial o la elaboración de perfiles por razones políticas;
 - al menoscabo de la libertad de prensa y de las comunicaciones con miembros de profesiones que gozan del privilegio de confidencialidad, incluidos los abogados y los médicos;
 - 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 las actividades policiales y de inteligencia, lo cual conlleva que todos los ciudadanos sean tratados como sospechosos y estén sometidos a vigilancia;
 - a las amenazas a la intimidad en una era digital **y *el impacto de la vigilancia masiva en ciudadanos y sociedades***;
- H. Considerando que la magnitud sin precedentes del espionaje revelado requiere una investigación completa por parte de las autoridades de los Estados Unidos, las instituciones europeas y los gobiernos, parlamentos nacionales y autoridades judiciales de los Estados miembros;
- I. 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 determinados Estados miembros de la UE; y que los gobiernos y parlamentos de la UE guardan silencio con demasiada frecuencia y no ponen en marcha investigaciones adecuadas;
- J. Considerando que el Presidente Obama anunció recientemente una reforma de la Agencia Nacional de Seguridad y de sus programas de vigilancia;
- K. Considerando que, en comparación con las acciones emprendidas tanto por las instituciones de la UE como por determinados Estados miembros de la UE, el Parlamento Europeo se ha tomado muy en serio su obligación de arrojar luz sobre las revelaciones de prácticas indiscriminadas de vigilancia masiva de ciudadanos de la UE y que, mediante 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,

encargó a su Comisión de Libertades Civiles, Justicia y Asuntos de Interior que llevara a cabo una investigación en profundidad de la cuestión;

- L. 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 validez jurídica de los tratados de la UE no sea menoscabada por una 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

- M. 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 estadounidense¹; que, no obstante, el tribunal de distrito del Distrito Sur de Nueva York sentenció, en su decisión de 27 de diciembre de 2013, que esta recopilación era legal;
- N. Considerando que una decisión del tribunal de distrito del Distrito Oriental de Michigan ha resuelto que la Cuarta Enmienda exige que todas las investigaciones sean razonables, que haya mandatos previos para toda investigación razonable, mandatos basados en causas probables existentes anteriormente, así como que las personas, lugares y objetos se especifiquen y que un magistrado neutral se interponga entre los agentes encargados de garantizar la ley y los ciudadanos²;
- O. Considerando que, en su informe de 12 de diciembre de 2013, el Grupo de Revisión del Presidente sobre Inteligencia y Tecnología de las Comunicaciones propone 46 recomendaciones al Presidente de los Estados Unidos; que las recomendaciones destacan la necesidad de proteger simultáneamente la seguridad nacional, la intimidad personal y las libertades civiles; y 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 Defensor del 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 de lucha contra el terrorismo; y a que reciba reclamaciones de denunciantes, haga uso de los Tratados de Asistencia Judicial Mutua y no utilice la vigilancia para sustraer secretos industriales o comerciales;
- P. Considerando que, según un memorando abierto presentado al Presidente Obama por antiguos altos ejecutivos de la Agencia Nacional de Seguridad (Veteran Intelligence Professionals for Sanity, VIPS) el 7 de enero de 2014³, la recopilación masiva de datos

¹ Klayman et al. contra Obama et al., acción civil n° 13-0851, 16 de diciembre de 2013.

² ACLU contra Agencia Nacional de Seguridad, n° 06-CV-10204, 17 de agosto de 2006.

³ <http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong>.

no mejora su capacidad para prevenir futuros ataques terroristas; considerando que los autores recalcan que la vigilancia masiva realizada por la Agencia Nacional de Seguridad ha prevenido cero ataques y que se han gastado miles de millones de dólares en programas que son menos eficaces e interfieren muchísimo más en la intimidad de los ciudadanos que una tecnología propia llamada THINTHREAD que se desarrolló en 2001;

- Q. Considerando que, con respecto a las actividades de inteligencia relativas a ciudadanos no estadounidenses llevadas a cabo en virtud de la sección 702 de la FISA, las recomendaciones al Presidente de los Estados Unidos reconocen el principio fundamental de respeto de la intimidad y la dignidad humana consagrado en el artículo 12 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;
- R. Considerando que, en su Directiva Presidencial sobre actividades de inteligencia de señales de 17 de enero de 2014 y en el correspondiente discurso, el Presidente de los Estados Unidos, Barack Obama, declaró que los Estados Unidos necesitan la vigilancia electrónica masiva a fin de salvaguardar su seguridad nacional y proteger a sus ciudadanos y a los ciudadanos de los aliados y socios de los Estados Unidos, así como para promover sus intereses en materia de política exterior; que esta Directiva Presidencial contiene determinados principios en cuanto a la recopilación, el uso y el intercambio de inteligencia de señales, y que hace extensivas determinadas salvaguardias a los ciudadanos no estadounidenses, estableciendo en parte un tratamiento equivalente al de los ciudadanos estadounidenses, incluidas salvaguardias para la información personal de todas las personas, independientemente de su nacionalidad o lugar de residencia; que, no obstante, el Presidente Obama no pidió propuestas concretas, especialmente en cuanto a la prohibición de las actividades de vigilancia masiva y a la introducción de la posibilidad de interposición de recursos administrativos y judiciales para las personas no estadounidenses;

Marco jurídico

Derechos fundamentales

- S. 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 los Estados Unidos, pero no ha logrado 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;
- T. 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 el Convenio Europeo de Derechos Humanos, constituyen piedras angulares de la democracia, y que la vigilancia masiva de seres humanos es incompatible con estas piedras angulares;

- U. Considerando que, en todos los Estados miembros, la legislación protege contra la revelación de la información comunicada de forma confidencial entre abogado y cliente, un principio que ha sido reconocido por el Tribunal de Justicia Europeo¹;
- V. Considerando que, en su Resolución de 23 de octubre de 2013 sobre la delincuencia organizada, la corrupción y el blanqueo de dinero, el Parlamento pedía a la Comisión que presentase una propuesta legislativa por la que se estableciese un programa europeo eficaz y global para la protección de denunciantes con objeto de proteger los intereses financieros de la UE y que, asimismo, examinase si dicha futura legislación debía también abarcar otros ámbitos de competencia de la Unión;

Competencias de la Unión Europea en materia de seguridad

- W. 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 es competente en asuntos de seguridad interna (artículo 4, letra j), del TFUE) y ha ejercido esta facultad decidiendo sobre varios instrumentos legislativos y celebrando acuerdos internacionales (PNR, TFTP) orientados a luchar contra los delitos graves y el terrorismo y creando una estrategia de seguridad interna y agencias que trabajan en este ámbito;
- X. Considerando que el Tratado de Funcionamiento de la Unión Europea establece que «los Estados miembros tendrán la posibilidad de organizar entre ellos y bajo su responsabilidad formas de cooperación y coordinación en la medida en que lo estimen apropiado, entre los servicios competentes de sus administraciones responsables de velar por la seguridad nacional» (artículo 73 del TFUE);
- Y. Considerando que el artículo 276 del TFUE establece que «en el ejercicio de sus atribuciones respecto de las disposiciones de los capítulos 4 y 5 del título V de la tercera parte relativas al espacio de libertad, seguridad y justicia, el Tribunal de Justicia de la Unión Europea no será competente para comprobar la validez o proporcionalidad de operaciones efectuadas por la policía u otros servicios con funciones coercitivas de un Estado miembro, ni para pronunciarse sobre el ejercicio de las responsabilidades que incumben a los Estados miembros respecto del mantenimiento del orden público y de la salvaguardia de la seguridad interior»;
- Z. 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;
- AA. Considerando que los Tratados Europeos confieren a la Comisión Europea el papel de «guardiana de los Tratados», y que, por consiguiente, es su responsabilidad legal

¹ Sentencia de 18 de mayo de 1982 en el asunto C-155/79, AM & S Europe Limited contra Comisión de las Comunidades Europeas.

investigar cualquier posible violación del Derecho de la UE;

- AB. Considerando que, de conformidad con el artículo 6 del TUE, que hace referencia a la Carta de los Derechos Fundamentales de la Unión Europea y al CEDH, las agencias e incluso los particulares de los Estados miembros que operen en el ámbito de la seguridad nacional también tienen que respetar los derechos allí consagrados, ya sean los de sus propios ciudadanos o los de ciudadanos de otros Estados;

Extraterritorialidad

- AC. Considerando que la aplicación extraterritorial por parte de un tercer país de sus leyes, legislaciones y otros instrumentos legislativos y ejecutivos en situaciones que estén dentro de la jurisdicción de la UE o de 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 dichas circunstancias, es necesario adoptar medidas a nivel de la Unión para garantizar el respeto dentro de la UE de los valores europeos consagrados en el artículo 2 del TUE, en la Carta de los Derechos Fundamentales de la Unión Europea y en el CEDH por lo que se refiere a los derechos fundamentales, la democracia y el Estado de Derecho, así como los derechos de las personas físicas y jurídicas consagrados en la legislación secundaria por la que se aplican estos principios fundamentales, por ejemplo, eliminando, neutralizando, bloqueando o luchando por otros medios contra los efectos de la legislación extranjera pertinente;

Transferencias internacionales de datos

- AD. 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 salvaguardias 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 Europea¹, de infracción del Derecho de la UE, que incluye cualquier infracción de los derechos fundamentales consagrados en la Carta de la UE;
- AE. Considerando que la transferencia de datos no está limitada geográficamente y, sobre todo en un contexto de globalización creciente y comunicación mundial, el legislador de la UE se enfrenta a nuevos retos en cuanto a la protección de los datos y las comunicaciones personales, y que por ello resulta de la máxima importancia que se fomenten marcos jurídicos sobre normas comunes;
- AF. Considerando que la recopilación masiva de datos personales con fines comerciales y en el marco de la lucha contra el terrorismo y los delitos transnacionales graves pone en peligro los derechos de los ciudadanos de la UE en relación con los datos personales y la

¹ Véanse especialmente los asuntos acumulados C-6/90 y C-9/90, Francovich y otros contra Italia, sentencia de 19 de noviembre de 1991.

intimidad;

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

- AG. Considerando que el marco jurídico de protección de datos de los EE.UU. no garantiza un nivel adecuado de protección para los ciudadanos de la UE;
- AH. 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 2000/520/CE, 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 los EE.UU. para los datos personales transferidos desde la Unión a organizaciones establecidas en los EE.UU. que cumplan con los principios de puerto seguro;
- AI. Considerando que, en su Resolución de 5 de julio de 2000, el Parlamento 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;
- AJ. Considerando que, en el documento de trabajo 4 del Parlamento sobre las 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, de 12 de diciembre de 2013, los ponentes expresaron dudas y preocupaciones acerca de la adecuación del puerto seguro y pidieron a la Comisión que derogara la decisión relativa a la adecuación del puerto seguro y encontrara nuevas soluciones jurídicas;
- AK. Considerando que la Decisión 2000/520/CE 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;
- AL. Considerando que la Decisión 2000/520/CE 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 alcance;
- AM. Considerando que, en sus dos primeros informes sobre la aplicación del puerto seguro, publicados en 2002 y 2004, la Comisión identificó varias deficiencias en lo que respecta a la adecuada aplicación del puerto seguro y realizó diversas recomendaciones a las autoridades estadounidenses con el fin de rectificar dichas deficiencias;
- AN. Considerando que, en su tercer informe de aplicación, de 27 de noviembre de 2013, nueve años después del segundo informe y sin que ninguna de las deficiencias reconocidas en dicho informe hubiese sido rectificadas, la Comisión identificó otros defectos y deficiencias 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 de 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 habrían de aplicarse lo antes posible, creando la base para una revisión total del funcionamiento de los principios de puerto seguro;

- AO. Considerando que, entre el 28 y el 31 de octubre de 2013, una delegación de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (Comisión LIBE) se reunió en Washington D.C. con el Departamento de Comercio y la Comisión Federal de Comercio de los Estados Unidos; que el Departamento de Comercio reconoció la existencia de organizaciones que han autocertificado su adhesión a los principios de puerto seguro pero cuya situación claramente no está actualizada, lo que significa que la empresa no cumple 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;
- AP. 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 considere necesario y proporcionado en una sociedad democrática, y que la ley debe establecer claramente las condiciones y garantías para que dicha limitación sea legítima; que los EE.UU. y la UE, y sobre todo la Comisión, deberían haber aclarado el ámbito de aplicación de dicha excepción, a fin de evitar cualquier interpretación o aplicación que anulase en esencia el derecho fundamental a la intimidad y la protección de datos, entre otros; y que, por consiguiente, dicha excepción no debe utilizarse de forma que menoscabe o anule la protección garantizada por la Carta de los Derechos Fundamentales de la Unión Europea, el CEDH, la legislación en materia de protección de datos de la UE y los principios de puerto seguro; insiste en que, si se invoca la excepción por motivos de seguridad nacional, debe especificarse en virtud de qué ley nacional;
- AQ. 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 cara a 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

- AR. 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, Canadá y Australia han participado en una vigilancia masiva a gran escala de comunicaciones electrónicas y han colaborado activamente con los Estados

Unidos en el programa denominado «Cinco Ojos» (Five Eyes), y pueden haber intercambiado recíprocamente datos personales de ciudadanos de la UE transferidos desde la UE;

- AS. Considerando que las Decisiones 2013/65/UE¹ y 2002/2/CE de la Comisión², han confirmado que la Ley sobre la vida privada de Nueva Zelanda y la Ley de Documentos Electrónicos y Protección de la Información Personal de Canadá garantizaban, respectivamente, un nivel adecuado de protección; 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

- AT. 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 del 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;
- AU. Considerando que estas garantías pueden, en particular, resultar de cláusulas contractuales pertinentes;
- AV. 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 que, sobre esta base, 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;
- AW. 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 normativa a la que están sujetos el importador de datos o un subencargado les exige que apliquen excepciones a la legislación en materia de protección de datos aplicable que van más allá de las restricciones necesarias en una sociedad democrática, como se establece en el artículo 13 de la Directiva 95/46/CE, cuando tales exigencias puedan tener un importante efecto negativo sobre las garantías previstas por la legislación en materia de protección de datos aplicable y las cláusulas contractuales tipo, o cuando exista una probabilidad sustancial de que estas 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;
- AX. 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; que, antes de que se puedan

¹ DO L 28 de 30.1.2013, p. 12.

² DO L 2 de 4.1.2002, p. 13.

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, y que las normas empresariales vinculantes para los encargados del tratamiento de datos han sido rechazadas en el informe de la Comisión LIBE sobre el Reglamento general de protección de datos, puesto que privarían al responsable del tratamiento de datos y al interesado de todo control sobre la jurisdicción en la que se tratan sus datos;

- AY. Considerando que el Parlamento Europeo, dada su competencia estipulada por el artículo 218 del TFUE, tiene la responsabilidad de revisar continuamente el valor de los acuerdos internacionales a los que ha concedido su aprobación;

Transferencias basadas en los acuerdos TFTP y PNR

- AZ. 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 TFTP, y en especial de su artículo 1;
- BA. Considerando que el seguimiento de la financiación del terrorismo constituye una herramienta esencial en la lucha contra la financiación del terrorismo y los delitos graves, ya que permite a los investigadores antiterroristas descubrir los vínculos entre los objetivos de investigación y otros sospechosos potenciales conectados con redes terroristas más amplias sospechosas de financiar el terrorismo;
- BB. Considerando que el Parlamento pidió a la Comisión que suspendiera el Acuerdo y solicitó que toda la información y los documentos relevantes estuvieran disponibles de inmediato para las deliberaciones del Parlamento; considerando que la Comisión no ha hecho ni lo uno ni lo otro;
- BC. Considerando que, a raíz de las alegaciones publicadas en los medios de comunicación, la Comisión decidió iniciar consultas con los 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 directa de datos contraria a las disposiciones del Acuerdo TFTP; considerando que no está claro si las autoridades estadounidenses han eludido el Acuerdo accediendo por otros medios a dichos datos, como indicaban en su carta de 18 de septiembre de 2013¹;

¹ La carta señala que «el Gobierno de los Estados Unidos busca y obtiene información financiera [...] (que) se recopila a través de canales reglamentarios, policiales, diplomáticos y de inteligencia, así como mediante intercambios con socios extranjeros» y que «el Gobierno de los Estados Unidos utiliza el TFTP para obtener datos SWIFT que no obtenemos por otras fuentes».

- BD. Considerando que, durante su visita a Washington de los días 28 a 31 de octubre de 2013, la delegación LIBE se reunió con el Departamento del Tesoro de los 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;
- BE. Considerando que, el 13 de noviembre de 2013, las autoridades de protección de datos de Bélgica y los Países Bajos 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 europeos¹;
- BF. 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 lucha contra el terrorismo y en consonancia con los términos específicos del Acuerdo;
- BG. 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 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

- BH. Considerando que el Acuerdo de asistencia judicial en materia penal entre la Unión Europea y los Estados Unidos, de 6 de junio de 2003², 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»)

- BI. 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 prevenir, investigar, descubrir y perseguir las infracciones penales, incluido el terrorismo, en el marco de la cooperación policial y judicial en materia penal; que las

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.

negociaciones fueron autorizadas por el Consejo el 2 de diciembre de 2010, y que este acuerdo reviste una enorme importancia, puesto que serviría de base para facilitar la transferencia de datos en el contexto de la cooperación policial y judicial, y en cuestiones penales;

- BJ. 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 judicial a sus datos personales, y a la rectificación y cancelación de los mismos, en los EE.UU., así como el derecho a un mecanismo de recurso administrativo y judicial eficaz para los ciudadanos de la UE en los EE.UU. y a una supervisión independiente de las actividades de tratamiento de datos;
- BK. 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;
- BL. Considerando que las negociaciones sobre el acuerdo no han avanzado debido a la persistente negativa por parte del Gobierno de los EE.UU. a 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

- BM. 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 datos¹, que sustituirá a la Directiva 95/46/CE y establecerá una legislación uniforme en toda la UE, y una Directiva², 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;
- BN. 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;
- BO. 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, tras dos años de deliberaciones, el Consejo todavía no ha sido capaz de lograr un enfoque general por lo que se refiere al Reglamento y a la Directiva general de protección de

¹ COM(2012)0011 de 25.1.2012.

² COM(2012)0010 de 25.1.2012.

datos¹;

Seguridad informática y computación en nube

- BP. Considerando que la mencionada Resolución de 10 de diciembre de 2013 destaca el potencial económico del negocio de la computación en nube para el crecimiento y el empleo, y que se prevé que el valor económico general del mercado de la nube tenga un valor anual de 207 000 millones de dólares estadounidenses en 2016, es decir, el doble de su valor en 2012;
- BQ. 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 nube que operan en la UE;
- BR. 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 o tratados de otra forma por los ciudadanos de la UE; que las autoridades de inteligencia estadounidenses han accedido a datos personales almacenados o tratados de otra forma en servidores ubicados en territorio estadounidense aprovechando las redes internas de Yahoo y de Google; que dichas actividades constituyen una violación de las obligaciones internacionales y normas europeas en materia de derechos fundamentales, incluidos el derecho a la vida privada y familiar, a la confidencialidad de las comunicaciones, a la presunción de inocencia, a la libertad de expresión, a la libertad de información, a la libertad de reunión y asociación y a la libertad de empresa; 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;
- BS. Considerando que las agencias de inteligencia de los Estados Unidos practican una política de menoscabo sistemático de los protocolos y los productos criptográficos a fin de poder interceptar incluso la comunicación cifrada; que la Agencia Nacional de Seguridad de los Estados Unidos ha recopilado cantidades ingentes de los llamados «ataques de día cero», vulnerabilidades de seguridad informática todavía desconocidas para el público o el vendedor del producto, y que tales actividades socavan masivamente los esfuerzos mundiales para mejorar la seguridad informática;
- BT. Considerando que el hecho de que las agencias de inteligencia hayan accedido a datos personales de usuarios de servicios en línea ha mermado gravemente la confianza de los ciudadanos en estos servicios y, por consiguiente, repercute negativamente en las empresas que invierten en el desarrollo de nuevos servicios que utilizan datos masivos (Big Data) y nuevas aplicaciones, como la «Internet de las Cosas»;
- BU. Considerando que los vendedores de tecnología informática a menudo suministran productos que no han sido debidamente probados en cuanto a su seguridad informática o que, a veces, incluso tienen puertas traseras incorporadas a propósito por el vendedor; que la falta de normas en materia de responsabilidad para los vendedores de software ha

¹ http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

provocado una situación que a su vez es explotada por las agencias de inteligencia, y que además entraña el riesgo de ataques por parte de otras entidades;

- BV. Considerando que es esencial que las empresas que proporcionan estos nuevos servicios y aplicaciones respeten las normas en materia de protección de datos y la intimidad de los interesados cuyos datos se recopilan, tratan y analizan, a fin de mantener un nivel elevado de confianza entre los ciudadanos;

Control democrático de los servicios de inteligencia

- BW. Considerando que a los servicios de inteligencia en las sociedades democráticas se les conceden poderes y capacidades especiales para proteger los derechos fundamentales, la democracia y el Estado de Derecho, los derechos de los ciudadanos y el Estado de las amenazas internas y externas, y que están sujetos a una rendición de cuentas democrática y un control judicial; considerando que, solo a tal efecto, se les otorgan dichos poderes y capacidades especiales, que se deben utilizar dentro de los límites legales impuestos por los derechos fundamentales, la democracia y el Estado de Derecho y cuya aplicación debe someterse a un escrutinio estricto, ya que, de lo contrario, pierden legitimidad y pudieran socavar la democracia;
- BX. Considerando que a los servicios de inteligencia se les concede un cierto nivel de secretismo para evitar que se pongan en peligro las operaciones en curso, se revelen los modos de actuación o corran peligro las vidas de los agentes, tal secretismo no puede invalidar o excluir las normas en materia de control y examen democrático y judicial de sus actividades, así como en materia de transparencia, sobre todo en relación con el respeto de los derechos fundamentales y el Estado de Derecho, todos ellos piedras angulares de una sociedad democrática;
- BY. 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 necesariamente adaptados a los rápidos avances tecnológicos de la última década, que han propiciado una cooperación internacional cada vez mayor en materia de inteligencia, también a través del intercambio a gran escala de datos personales, difuminando a menudo la frontera entre las actividades de inteligencia y las coercitivas;
- BZ. Considerando que el control democrático de las actividades de inteligencia sigue realizándose únicamente 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;
- CA. Considerando que los organismos nacionales de control a menudo no tienen pleno acceso a la inteligencia recibida de una agencia extranjera de inteligencia, lo que puede provocar lagunas que pueden propiciar que se lleven a cabo intercambios internacionales de información sin un examen adecuado; y que este problema se ve agravado por la denominada «norma de la tercera parte» o el principio de «control por el emisor», que ha sido diseñado para que el emisor mantenga el control sobre la divulgación ulterior de su información sensible, aunque por desgracia a menudo también se interprete como aplicable a la supervisión de los servicios destinatarios;

- CB. Considerando que las iniciativas públicas y privadas de reforma de la transparencia son fundamentales para garantizar la confianza del público en las actividades de las agencias de inteligencia, y que los sistemas jurídicos no deben impedir que las empresas revelen al público información acerca de cómo gestionan todo tipo de peticiones gubernamentales y órdenes judiciales de acceso a datos de los usuarios, incluida la posibilidad de revelar información agregada sobre el número de peticiones y órdenes aprobadas y rechazadas;

Principales conclusiones

1. Considera que las recientes revelaciones en la prensa por parte de denunciantes y periodistas, junto con las pruebas periciales proporcionadas durante esta investigación, el reconocimiento por parte de las autoridades y la insuficiente respuesta a estas acusaciones, 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 de comunicaciones, incluidos datos de contenido y datos y metadatos de 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 los programas de inteligencia de la Agencia Nacional de Seguridad estadounidense que permiten la vigilancia masiva de ciudadanos de la UE mediante un 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 la actividad preliminar de vigilancia (programa Tempora), el programa de descifrado (Edgehill), los ataques selectivos con intermediarios contra sistemas de información (programas Quantumtheory y Foxacid) y la recopilación y retención de 200 millones de mensajes de texto al día (programa Dishfire);
3. Toma nota de las presuntas actividades de «pirateo» o interceptación en los sistemas Belgacom de la agencia de inteligencia británica GCHQ; toma nota de las declaraciones de Belgacom de que no podía ni confirmar ni desmentir que las instituciones de la UE estuvieran afectadas o fueran objetivo de actividades de piratería, y que el software malicioso utilizado era extremadamente complejo y que su desarrollo y uso requerirían amplios recursos financieros y de personal que no estarían al alcance de entidades privadas o piratas informáticos;
4. Reitera que la confianza se ha visto profundamente afectada: la confianza entre ambos socios trasatlánticos, la confianza entre los ciudadanos y sus gobiernos, la confianza en el funcionamiento de las instituciones democráticas a ambas orillas del Atlántico, la confianza en el respeto del Estado de Derecho y la confianza en la seguridad de los servicios informáticos y las comunicaciones; cree que, para restablecer la confianza en todas estas dimensiones, se requiere un plan de actuación inmediato y exhaustivo que abarque una serie de medidas sujetas a control público;
5. Señala que varios gobiernos argumentan que estos programas de vigilancia masiva son necesarios para combatir el terrorismo; denuncia enérgicamente el terrorismo, pero cree firmemente que la lucha contra el terrorismo nunca puede constituir una justificación

para llevar a cabo programas de vigilancia masiva no selectivos, secretos o, incluso, ilegales; opina que dichos programas son incompatibles con los principios de necesidad y proporcionalidad en una sociedad democrática;

6. Recuerda la firme convicción de la UE de que es necesario encontrar el justo equilibrio entre las medidas de seguridad y la protección de las libertades civiles y los derechos fundamentales, al tiempo que se garantiza el máximo respeto por la vida privada y la protección de datos;
7. Considera que una recopilación de datos de semejante magnitud suscita considerables dudas sobre si estas acciones se guían únicamente 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 fines, incluido el espionaje político y económico, que deben ser disipados de forma exhaustiva;
8. 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, así como 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»;
9. 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 o una rendición de cuentas democrática;
10. Condena la recopilación generalizada extensa y sistemática de los 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 en 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 repercute de manera potencialmente grave en la libertad de prensa, de pensamiento y de expresión y en la libertad de reunión y asociación, e implica un potencial significativo para el uso abusivo de la información recogida contra adversarios políticos; enfatiza que estas actividades de vigilancia masiva también implican acciones ilegales por parte de los servicios de inteligencia y plantean interrogantes por lo que se refiere a la extraterritorialidad de las legislaciones nacionales;
11. Opina que es fundamental que el privilegio de confidencialidad profesional de los abogados, periodistas, médicos y otras profesiones reguladas se salvaguarde de las actividades de vigilancia masiva; subraya, en particular, que cualquier inseguridad sobre la confidencialidad de las comunicaciones entre los abogados y sus clientes podría repercutir negativamente en el derecho de los ciudadanos de la UE al acceso a asesoramiento jurídico y a la justicia y en el derecho a un juicio justo;
12. Considera que los programas de vigilancia constituyen un paso más hacia el establecimiento de un estado preventivo de pleno derecho, que cambie el paradigma establecido de Derecho penal en las sociedades democráticas según el cual cualquier interferencia con los derechos fundamentales de los sospechosos ha de ser autorizada

por un juez o fiscal sobre la base de una sospecha razonable y debe ser regulada por ley, y promoció en su lugar una mezcla de actividades policiales y de inteligencia con garantías jurídicas difuminadas y debilitadas, que a menudo no se ajustan a los controles y equilibrios democráticos y a los derechos fundamentales, especialmente la presunción de inocencia; recuerda, a este respecto, la decisión del Tribunal Constitucional Federal alemán¹ 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;

13. Se muestra convencido de que las leyes y los 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, la transferencia de datos personales puede ser reconocida o ejecutada en modo alguno salvo que exista un tratado de asistencia jurídica mutua o un acuerdo internacional en vigor entre el tercer país requirente y la Unión o un Estado miembro y una autorización previa por parte de la autoridad supervisora competente; recuerda que no deberá reconocerse ni ejecutarse ninguna sentencia de una corte o un tribunal secreto ni ninguna decisión de una autoridad administrativa de un Estado no perteneciente a la UE que, de forma secreta, autorice, directa o indirectamente, actividades de vigilancia;
14. Señala que las inquietudes anteriormente mencionadas se ven acentuadas por los rápidos avances tecnológicos y sociales, dado que Internet y los dispositivos móviles son omnipresentes en la vida 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; considera que la escala del problema no tiene precedentes; señala que se puede crear una situación en la que la infraestructura para la recopilación y el tratamiento masivos de datos podría utilizarse de forma abusiva en casos de cambio del régimen político;
15. Señala que no es posible garantizar, ni a las instituciones públicas de la UE ni a sus ciudadanos, que su seguridad o intimidad informática puedan ser protegidas de los ataques de intrusos bien equipados («falta de seguridad informática al 100 %»); advierte que, para alcanzar una seguridad informática máxima, los europeos deben estar dispuestos a dedicar suficientes recursos, tanto humanos como financieros, a conservar la independencia y autonomía de Europa en el ámbito de la tecnología informática;
16. Rechaza enérgicamente la idea de que todos los asuntos relacionados con programas de vigilancia masiva sean meramente una cuestión de seguridad nacional y, por lo tanto, de competencia exclusiva de los Estados miembros; reitera que los Estados miembros que respeten plenamente la legislación de la UE y el CEDH, al tiempo que toman medidas para garantizar su seguridad nacional; 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»²; recuerda, asimismo, que está en juego la protección de la intimidad de todos los ciudadanos de la UE, así como la seguridad y

¹ N° 1 BvR 518/02 de 4 de abril de 2006.

² Sentencia en el Asunto C-300/11, ZZ contra Secretario de Estado del Ministerio del Interior, 4 de junio de 2013.

fiabilidad de todas las redes de comunicación de la UE; cree, por 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 de la UE;

17. 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;
18. 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 un mecanismo de seguimiento en la próxima legislatura que garantice que las conclusiones ocupan un lugar predominante en la agenda política de la UE;
19. Tiene intención de exigir a la nueva Comisión que se designará después de las elecciones europeas de mayo de 2014 un compromiso político firme para con la aplicación de las propuestas y recomendaciones de la presente investigación;

Recomendaciones

20. Pide a las autoridades estadounidenses y a los Estados miembros de la UE que aún no lo hayan hecho que prohíban las actividades de vigilancia masiva generalizada;
21. Pide a todos los Estados miembros de la UE, y en particular a los que participan en los llamados programas «Nueve Ojos» y «Catorce Ojos»¹, que evalúen exhaustivamente y, si procede, revisen sus legislaciones y prácticas nacionales por las que se rigen las actividades de los servicios de inteligencia con el fin de garantizar que estén sujetas a control parlamentario, judicial y público, que respeten los principios de legalidad, necesidad, proporcionalidad, garantías procesales, notificación al usuario y transparencia, inclusive con referencia a la Recopilación de buenas prácticas de las Naciones Unidas y las recomendaciones de la Comisión de Venecia, y que se atengan a los estándares del Convenio Europeo de Derechos Humanos y cumplan con sus obligaciones en materia de derechos fundamentales, en particular por lo que se refiere a la protección de datos, la intimidad y la presunción de inocencia;
22. Pide a todos los Estados miembros de la UE y, en particular, en consideración de su Resolución de 4 de julio de 2013 y de sus vistas de investigación, al Reino Unido, Francia, Alemania, Suecia, los Países Bajos y Polonia, que se aseguren de que todos sus marcos legislativos y mecanismos de control actuales y futuros por las que se rigen las actividades de los servicios de inteligencia se atengan a los estándares del Convenio Europeo de Derechos Humanos y a la legislación en materia de protección de datos de la Unión Europea; invita a dichos Estados miembros a aclarar las acusaciones de actividades de vigilancia masiva, incluida la vigilancia masiva de telecomunicaciones transfronterizas, la vigilancia indiscriminada de las comunicaciones por cable, posibles

¹ El programa «Nueve Ojos» incluye a los EE.UU, el Reino Unido, Canadá, Australia, Nueva Zelanda, Dinamarca, Francia, Noruega y los Países Bajos; el programa «Catorce Ojos» incluye a dichos países y también a Alemania, Bélgica, Italia, España y Suecia.

- acuerdos entre servicios de inteligencia y empresas de telecomunicaciones en lo que respecta al acceso e intercambio de datos personales y el acceso a los cables transatlánticos, la presencia de equipos y personal de inteligencia estadounidenses en territorio de la UE sin control sobre las operaciones de vigilancia, y la compatibilidad de las mismas con la legislación de la UE; invita a los parlamentos nacionales de esos países a intensificar la cooperación de sus organismos de control de los servicios de inteligencia a nivel europeo;
23. Pide al Reino Unido, en particular, y dados los amplios informes de los medios de comunicación que hacen referencia a la vigilancia masiva de los servicios de inteligencia del GCHQ, que revise su actual marco jurídico, integrado por una «compleja interacción» entre tres actos legislativos diferentes (la Ley de derechos humanos de 1998, la Ley de Servicios de Inteligencia de 1994 y la Ley de regulación de las facultades de investigación de 2000);
 24. Toma nota de la revisión de la Ley neerlandesa sobre Inteligencia y Seguridad de 2002 (Informe de la Comisión Dessens de 2 de diciembre de 2013); apoya las recomendaciones de la comisión de revisión que tienen por objeto reforzar la transparencia, el control y la supervisión de los servicios neerlandeses de inteligencia; pide a los Países Bajos que se abstengan de ampliar las competencias de los servicios de inteligencia de tal manera que también se pueda realizar una vigilancia indiscriminada y a gran escala en comunicaciones por cable de ciudadanos inocentes, especialmente dado que uno de los mayores Puntos de Intercambio de Internet del mundo está ubicado en Amsterdam (AMS-IX); pide prudencia a la hora de definir el mandato y las capacidades de la nueva Unidad de Ciberinteligencia de Señales Conjunta (Joint Sigint Cyber Unit), así como en lo concerniente a la presencia y actividad de personal estadounidense de inteligencia en territorio neerlandés;
 25. Solicita a los Estados miembros, también cuando estén representados por sus agencias de inteligencia, que se abstengan de aceptar datos de terceros países que hayan sido recopilados ilegalmente, así como 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 TUE, del CEDH y de la Carta de los Derechos Fundamentales de la UE;
 26. Reclama que se ponga fin a la interceptación y tratamiento a gran escala de las imágenes de cámaras web por parte de todos los servicios secretos; pide a los Estados miembros que investiguen a fondo cómo y en qué medida sus respectivos servicios secretos han intervenido en la recogida y tratamiento de las imágenes de cámaras web y que destruyan todas las imágenes almacenadas que hayan sido recogidas a través de esos programas de vigilancia a gran escala;
 27. 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 o por sus propios servicios de inteligencia, y garanticen que el Estado de Derecho no se vea debilitado por la aplicación extraterritorial de la legislación de un tercer país;
 28. 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»;

29. 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 que hagan uso de todas las medidas internacionales disponibles para defender los derechos fundamentales de los ciudadanos de la UE, 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 (PIDCP);
30. Pide a los Estados miembros que prevean mecanismos efectivos para que respondan de ese abuso de poder las personas responsables de los programas de vigilancia (a gran escala) que han vulnerado las normas del Estado de Derecho y los derechos fundamentales de los ciudadanos;
31. 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 de la UE, proporcionen vías de recurso jurisdiccional para los ciudadanos de la UE, pongan los derechos de los ciudadanos de la UE en el mismo plano que los derechos de los ciudadanos de los EE.UU. y suscriban el Protocolo Opcional que permite las denuncias individuales en virtud del PIDCP;
32. Aplaude, en este sentido, las observaciones realizadas y la Directiva Presidencial emitida por el Presidente Obama el 17 de enero de 2014, en tanto que paso hacia la limitación de la autorización del uso de vigilancia y tratamiento de datos para fines de seguridad nacional y hacia la igualdad de trato de la información personal de todas las personas, independientemente de su nacionalidad o residencia, por parte de la comunidad de inteligencia de los EE.UU.; espera, no obstante, en el contexto de las relaciones UE-EE.UU., más pasos específicos que, ante todo, reforzarán la confianza en las transferencias transatlánticas de datos y ofrecerán garantías vinculantes para unos derechos a la intimidad que los ciudadanos de la UE puedan hacer valer, tal como se describe en detalle en el presente informe;
33. Hace hincapié en su gran preocupación por los trabajos realizados en el seno del Consejo de Europa por el Comité del Convenio sobre la Ciberdelincuencia por lo que se refiere a la interpretación del artículo 32 del Convenio sobre Ciberdelincuencia de 23 de noviembre de 2001 (Convenio de Budapest) en lo concerniente al acceso transfronterizo a los datos informáticos almacenados con autorización o públicamente disponibles, y se opone a la conclusión de un protocolo adicional u orientación que pretenda ampliar el alcance de esta disposición más allá del actual régimen establecido por dicho Convenio, que ya constituye una importante excepción al principio de territorialidad porque podría resultar en el acceso remoto sin restricciones por parte de las autoridades policiales a servidores y ordenadores ubicados en otras jurisdicciones sin recurso a acuerdos de asistencia judicial mutua y otros instrumentos de cooperación judicial establecidos para garantizar los derechos fundamentales de la persona, incluida la protección de datos y las garantías procesales, y en particular el Convenio n° 108 del Consejo de Europa;
34. Pide a la Comisión que, antes de julio de 2014, efectúe una evaluación de la

aplicabilidad del Reglamento (CE) nº 2271/96 a los casos de conflictos de leyes en las transferencias de datos personales;

35. Pide a la Agencia de Derechos Fundamentales que lleve a cabo una investigación en profundidad sobre la protección de los derechos fundamentales en el contexto de la vigilancia y, en especial, sobre la situación jurídica actual de los ciudadanos de la UE por lo que respecta a los recursos judiciales de que disponen en relación con dichas prácticas;

Transferencias internacionales de datos

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

36. 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 (por ejemplo, Google, Microsoft, Yahoo!, Facebook, Apple y LinkedIn); expresa su preocupación por el hecho de que estas organizaciones no hayan cifrado ni la información ni las comunicaciones que fluyen entre sus centros de datos, permitiendo de ese modo a los servicios de inteligencia interceptar información; aplaude las consiguientes declaraciones realizadas por algunas empresas estadounidenses de que van a acelerar los planes para cifrar los flujos de datos entre sus centros de datos mundiales;
37. 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 los criterios de exención en materia de seguridad nacional;
38. Opina que, en vista de que los principios de puerto seguro no proporcionan una protección adecuada a los ciudadanos de la UE en las circunstancias actuales, estas transferencias deben realizarse con arreglo a otros instrumentos, como cláusulas contractuales o normas empresariales vinculantes, siempre que dichos instrumentos establezcan garantías y protecciones específicas que no sean eludidas por otros instrumentos jurídicos;
39. Opina que la Comisión no ha actuado para solucionar las conocidas deficiencias de la actual aplicación del puerto seguro;
40. Pide a la Comisión que presente medidas que prevean la suspensión inmediata de la Decisión 2000/520/CE 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; invita, por tanto, a las autoridades estadounidenses a que presenten un propuesta para un nuevo marco para las transferencias de datos personales de la UE a los EE.UU. que cumpla los requisitos de la legislación de la Unión en materia de protección de datos y proporcione el adecuado nivel de protección requerido;
41. Pide a las autoridades competentes de los Estados miembros, y en particular a las autoridades responsables de la protección de datos, que utilicen los poderes de que

disponen 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 salvaguardias necesarias con respecto a la protección de la intimidad y los derechos y libertades fundamentales de las personas;

42. Invita a la Comisión a que, antes de diciembre de 2014, presente una evaluación exhaustiva del marco en materia de protección de la intimidad de los EE.UU. que cubra las actividades comerciales, policiales y de inteligencia, así como recomendaciones concretas basadas en la ausencia de una ley general de protección de datos en los EE.UU.; alienta a la Comisión a entablar negociaciones con la administración estadounidense con objeto de establecer un marco jurídico que proporcione un elevado nivel de protección de los individuos por lo que respecta a la protección de sus datos de carácter personal cuando sean transferidos a los EE.UU., así como a garantizar la equivalencia de los marcos en materia de protección de la intimidad de la UE y los EE.UU.;

Transferencias a otros terceros países con la decisión de adecuación

43. 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;
44. Recuerda que la Directiva 95/46/CE prevé igualmente que la adecuación del nivel de protección conferido por un tercer país debe ser evaluada a la luz de todas las circunstancias que rodean a la operación de transferencia de los datos o al conjunto de tales operaciones; recuerda asimismo que dicha Directiva también dota a la Comisión de poderes 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; evoca que la Directiva 95/46/CE también faculta a la Comisión a declarar que un tercer país no garantiza un adecuado nivel de protección;
45. 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;
46. Pide a la Comisión y a los Estados miembros que evalúen sin demora si el nivel de protección adecuado de la Ley sobre la vida privada de Nueva Zelanda y la Ley de Documentos Electrónicos y Protección de la Información Personal de Canadá, según se declara en las Decisiones 2013/65/UE y 2002/2/CE de la Comisión, se ha visto afectado por la participación de las agencias nacionales de inteligencia de ambos países en la vigilancia masiva de ciudadanos de la UE y que, si procede, tomen las medidas oportunas para suspender o revertir las decisiones de adecuación; pide asimismo a la Comisión que evalúe la situación de los restantes países que han recibido una clasificación de adecuación; confía en que la Comisión informe al Parlamento de sus conclusiones sobre los países antes citados para diciembre de 2014, a más tardar;

Transferencias basadas en cláusulas contractuales y otros instrumentos

47. 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;
48. 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 resulte probable que la ley a la que está sometido el destinatario de los datos le impone requisitos que van más allá de las restricciones estrictamente necesarias, adecuadas y proporcionadas en una sociedad democrática y que pueden tener un efecto negativo sobre las garantías previstas por la legislación en materia de protección de datos aplicable y las cláusulas contractuales tipo, o cuando la continuación de la transferencia pudiera provocar un riesgo de daños graves para los interesados;
49. 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 libertades de las personas, teniendo en cuenta especialmente las leyes en materia de inteligencia y seguridad nacional de terceros países y la participación de las empresas que reciben los datos en un tercer país en actividades de vigilancia masiva por parte de las agencias de inteligencia de un tercer país;
50. Pide a la Comisión que examine sin demora 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

51. Pide a la Comisión que realice, antes de que finalice 2014, una evaluación en 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 también 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; pide igualmente al Consejo y a la Comisión que evalúen los Acuerdos bilaterales entre los Estados Miembros y los Estados Unidos con

el fin de velar por la congruencia entre dichos acuerdos bilaterales y los que la UE mantiene o decida mantener con los Estados Unidos;

Asistencia judicial en materia penal en la UE

52. Pide al Consejo y a la Comisión que informen al Parlamento sobre el uso real que hacen los Estados miembros del Convenio relativo a la asistencia judicial 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

53. 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 tener que recurrir a los canales bilaterales existentes para la asistencia y la cooperación judiciales mutuas;
54. Reitera su Resolución de 23 de octubre de 2013 y pide a la Comisión que suspenda el acuerdo TFTP;
55. Pide a la Comisión que reaccione ante las inquietudes que suscita el hecho de que tres de los principales sistemas informatizados de reserva 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 con arreglo a 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»)

56. Considera que una solución satisfactoria a tenor del «acuerdo marco» constituye una condición previa para la completa recuperación de la confianza entre los socios transatlánticos;
57. Pide la inmediata reanudación de las negociaciones con los Estados Unidos en relación con el «acuerdo marco», que debe poner los derechos de los ciudadanos europeos en el mismo plano que los derechos de los ciudadanos estadounidenses; subraya, además, que dicho acuerdo debe proporcionar recursos administrativos y judiciales eficaces y aplicables a todos los ciudadanos de la UE en los Estados Unidos, sin discriminación alguna;
58. 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 con los EE.UU. hasta que el «acuerdo marco» no haya entrado en vigor;
59. 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

60. Pide a la Presidencia del Consejo y a los Estados miembros que aceleren su labor en relación con la totalidad del paquete de protección de datos para permitir su adopción en 2014, de modo que los ciudadanos de la UE puedan disfrutar de un nivel elevado de protección de sus datos en un futuro muy cercano; subraya que un compromiso firme y pleno apoyo por parte del Consejo son condiciones necesarias para demostrar credibilidad y autoridad frente a terceros países;
61. 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, ambos 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; hace hincapié en que únicamente adoptará nuevas medidas de cooperación policial cuando el Consejo inicie negociaciones con el Parlamento y la Comisión sobre el paquete de protección de datos;
62. Recuerda que los conceptos de «protección de la intimidad desde el diseño» y «protección de la intimidad por defecto» constituyen un refuerzo de la protección de datos y que deben servir de líneas directrices para todos los productos, servicios y sistemas ofrecidos en internet;
63. Considera que unas normas de transparencia y seguridad más estrictas para internet y para las telecomunicaciones son un principio necesario para mejorar el sistema de protección de datos, por lo que pide a la Comisión que presente una propuesta legislativa sobre términos y condiciones generales y estandarizados para los servicios en línea y de telecomunicaciones, así como que encargue a un organismo de supervisión que controle la conformidad con dichos términos y condiciones generales;

Computación en nube

64. Señala que la confianza en la computación en nube estadounidense y en sus proveedores se ha visto negativamente afectada por las prácticas arriba indicadas; enfatiza, por tanto, que el desarrollo de soluciones informáticas y servicios en nube europeos constituye un elemento esencial para el crecimiento y el empleo y para la confianza en los servicios y proveedores de computación en nube, así como para garantizar un nivel elevado de protección de los datos personales;
65. Pide a todos los organismos públicos de la Unión que no empleen servicios en nube en aquellos casos en los que puedan resultar de aplicación disposiciones legislativas de fuera de la UE;
66. 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 servicios 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, así como por el acceso remoto directo a los datos e información personales tratados por las autoridades policiales y los servicios de inteligencia de

terceros países;

67. Lamenta 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;
68. Pide a la Comisión y a los Estados miembros que aceleren el establecimiento de la Asociación Europea de Computación en Nube, al tiempo que incluyen plenamente a la sociedad civil y a la comunidad técnica, como el Grupo Especial sobre Ingeniería de Internet (IETF), e incorporan elementos de protección de datos;
69. Insta a la Comisión a que, cuando negocie acuerdos internacionales que impliquen el tratamiento de datos personales, tome nota en particular de los riesgos y problemas asociados a la «computación en nube» para los derechos fundamentales, y en particular, pero no exclusivamente, para el desarrollo del derecho a la intimidad y la protección de datos personales, consagrado en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea; insta asimismo a la Comisión a que tome nota de las normas nacionales del socio negociador que rigen el acceso de las fuerzas del orden y los servicios de inteligencia a los datos personales tratados a través de servicios de computación en nube, en particular exigiendo que solo pueda concederse dicho acceso dentro del pleno respeto de las debidas garantías procesales y con arreglo a un fundamento jurídica inequívoco y que se especifiquen las condiciones exactas de acceso, la finalidad de tal acceso, las medidas de seguridad aplicadas en la transferencia de datos y los derechos del individuo, así como las normas de supervisión y un mecanismo de recurso efectivo;
70. Recuerda que todas las empresas que ofrezcan servicios en la UE deben cumplir sin excepción el Derecho de la UE y son responsables de las infracciones que cometan, y hace hincapié en la importancia de contar con sanciones administrativas efectivas, proporcionadas y disuasorias que puedan aplicarse a los proveedores de servicios de computación en nube que no respeten las normas de protección de datos de la UE;
71. Pide a la Comisión y a las autoridades competentes de los Estados miembros que evalúen la medida en la que se han infringido las normas de la UE sobre intimidad y protección de datos a través de la cooperación de las entidades jurídicas de la UE con servicios secretos, o al haberse acatado mandamientos judiciales de autoridades de terceros países solicitando datos personales de ciudadanos de la UE, en contravención de la legislación de la UE en materia de protección de datos;
72. Pide a aquellas empresas que presten nuevos servicios utilizando datos masivos y nuevas aplicaciones, como el «Internet de las Cosas», que elaboren medidas de protección de datos desde la fase de desarrollo a fin de mantener un nivel de confianza elevado entre los ciudadanos;

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

73. Reconoce que la UE y los Estados Unidos están negociando un Acuerdo de Asociación Transatlántica para el Comercio y la Inversión, que constituye una herramienta de importancia estratégica capital para crear más crecimiento económico;

74. 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 la aprobación por parte del Parlamento Europeo de la versión definitiva del Acuerdo ATCI podría correr peligro hasta que no cesen por completo las actividades de vigilancia masiva generalizada y la interceptación de comunicaciones en las instituciones y representaciones diplomáticas de la UE y no se encuentre una solución adecuada para los derechos de privacidad de datos de los ciudadanos de la UE, incluido el recurso administrativo y judicial; destaca que el Parlamento únicamente concederá su aprobación a la versión final del Acuerdo ATCI en caso de que dicho acuerdo respete, entre otras cosas, los derechos fundamentales reconocidos por la Carta de la UE, y siempre que la protección de la intimidad de las personas en relación con el procesamiento y la divulgación de datos personales sigan rigiéndose por el artículo XIV del AGCS; hace hincapié en que la legislación en materia de protección de datos de la UE no puede ser considerada una «discriminación arbitraria o injustificable» en la aplicación del artículo XIV del AGCS;

Control democrático de los servicios de inteligencia

75. 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 actuales organismos de control de la UE y de los Estados Unidos carecen de ambos, en especial de capacidades técnicas;
76. Invita, como ya hiciera 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 dispongan de recursos, pericia técnica y medios legales suficientes, incluido el derecho a realizar visitas *in situ*, para que puedan controlar los servicios de inteligencia de manera efectiva;
77. Pide que se cree un grupo de diputados y expertos para examinar, de manera transparente y en colaboración con los Parlamentos nacionales, recomendaciones con miras a una mejora del control democrático, incluido el control parlamentario, de los servicios de inteligencia, y a una mayor colaboración en materia de supervisión en la UE, en particular por lo que respecta a su dimensión transfronteriza; considera que el grupo debe examinar, en particular, la posibilidad de contar con directrices o normas mínimas europeas por lo que se refiere al control (ex ante y ex post) de los servicios de inteligencia sobre la base de las mejores prácticas y recomendaciones existentes de organismos internacionales (las Naciones Unidas, el Consejo de Europa), incluida la cuestión de que los organismos de supervisión sean considerados terceros a tenor de la «norma de la tercera parte» o el principio de control por el emisor, en relación con el control y la rendición de cuentas de la inteligencia procedente de países extranjeros, criterios para una mejor transparencia a partir del principio general de acceso a la información y de los llamados «Principios de Tshwane»¹, así como principios por lo que se refiere a los límites relativos a la duración y el alcance de cualquier vigilancia, para

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.

garantizar que sean proporcionados y se limiten a su fin;

78. Pide al grupo que elabore un informe para una conferencia que deberá celebrar el Parlamento con los organismos nacionales de control, ya sean parlamentarios o independientes, de aquí a principios de 2015, y que contribuya a la preparación de dicha conferencia;
79. 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;
80. 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);
81. Insta a la AR/VP a que informe regularmente de las actividades del Centro de Análisis de Inteligencia de la UE (IntCen), que forma parte del Servicio Europeo de Acción Exterior, a los organismos responsables del Parlamento, incluido el pleno respeto por su parte de los derechos fundamentales y de las normas sobre privacidad de datos aplicables de la UE, permitiendo un mejor control por el Parlamento de la dimensión exterior de las políticas de la UE; insta a la Comisión y a la AR/VP a que presenten una propuesta de marco jurídico para las actividades del IntCen, en caso de que se prevea alguna operación o futura competencia en materia de inteligencia o instrumento propio de recopilación de datos que pueda repercutir en la estrategia de seguridad interna de la UE;
82. Solicita a la Comisión que presente, antes de diciembre de 2014, una propuesta de procedimiento de habilitación de seguridad de la UE para todos los titulares de cargos de la UE, ya que el sistema actual, que se basa en la habilitación de seguridad del Estado miembro del que se tiene nacionalidad, establece 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;
83. 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 deberían emplearse para mejorar el control a nivel de la UE;

Agencias de la UE

84. 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 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; considera que Europol no debe tratar información o datos obtenidos mediante una violación de derechos fundamentales que estarían protegidos por la Carta de los Derechos Fundamentales;

85. Invita a Europol a hacer pleno uso de su mandato para solicitar a las autoridades competentes de los Estados miembros que emprendan investigaciones penales sobre ataques cibernéticos y delitos informáticos de gran calado con un posible impacto transfronterizo; considera que el mandato de Europol debería mejorarse con el fin de que esté capacitado para iniciar su propia investigación a raíz de la sospecha de un ataque malicioso contra los sistemas de redes e informáticos de dos o más Estados miembros u organismos de la Unión¹; pide a la Comisión que revise las actividades del Centro Europeo de Ciberdelincuencia de Europol y que, si procede, presente una propuesta para un marco integral a fin de reforzar las competencias del mismo;

Libertad de expresión

86. Expresa una gran preocupación por las crecientes amenazas que se ciernen sobre la libertad de prensa y el efecto amedrentador de la intimidación de las autoridades gubernamentales 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»;
87. Toma nota de la detención de David Miranda y de la incautación del material que obraba en su poder por las autoridades del Reino Unido de conformidad con el apéndice 7 de la Ley antiterrorista de 2000 (y también del requerimiento al periódico *The Guardian* para que destruyese o entregase el material), y manifiesta su preocupación de que ello constituye una posible interferencia grave con el derecho a la libertad de expresión y a la libertad de prensa reconocido en el artículo 10 de la CEDH y el artículo 11 de la Carta de la UE y de que la legislación en materia de lucha contra el terrorismo podría sufrir abusos en tales casos;
88. Llama la atención sobre la difícil situación de los denunciantes y sus partidarios, incluidos los periodistas, tras las revelaciones; pide a la Comisión que realice un examen para determinar si una futura propuesta legislativa por la que se estableciese un programa europeo eficaz y global para la protección de denunciantes, como ya solicitó en su Resolución de 23 de octubre de 2013, debería también abarcar otros ámbitos de competencia de la Unión, prestando especial atención a la complejidad que reviste la denuncia de irregularidades en el ámbito de la inteligencia; pide a los Estados miembros que estudien detenidamente la posibilidad de conceder a los denunciantes protección internacional contra el enjuiciamiento;
89. Pide a los Estados miembros que garanticen que su legislación, en particular en el ámbito de la seguridad nacional, ofrece una alternativa segura al silencio para la exposición o denuncia de irregularidades, incluidos corrupción, delitos penales,

¹ Posición del Parlamento Europeo de 25 de febrero de 2014 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia de la Unión Europea para la cooperación y la formación en funciones coercitivas (Europol) (Textos Aprobados, P7_TA(2014)0121).

infracciones de las obligaciones legales, errores judiciales y abuso de autoridad, que se ajuste asimismo a las disposiciones de los distintos instrumentos internacionales (Naciones Unidas y Consejo de Europa) de lucha contra de la corrupción, a los principios establecidos en la Resolución 1729 (2010) de la Asamblea Parlamentaria del Consejo de Europa, a los principios de Tshwane, etc.;

Seguridad informática de la UE

90. 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 y programas maliciosos; incide en que estos ataques precisan de unos recursos humanos y financieros a una escala tal que es probable que tengan su origen en entes estatales que actúen en nombre de gobiernos extranjeros; en este contexto, considera el caso de la piratería o interceptación de la empresa de telecomunicaciones Belgacom un preocupante ejemplo de un ataque contra la capacidad informática de la UE; subraya que el refuerzo de la capacidad y la seguridad informáticas de la UE también reducen la vulnerabilidad de la UE ante ataques cibernéticos graves a manos de organizaciones delictivas de gran tamaño o grupos terroristas;
91. 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, como medida estratégica de la máxima prioridad, una capacidad sólida y autónoma de recursos informáticos fundamentales; hace hincapié en que, para recuperar la confianza, esta capacidad informática europea debe basarse, en la medida de lo posible, en normas abiertas y en un software de código abierto y, a ser posible, en un hardware de las mismas características, de manera que la totalidad de la cadena de suministro, desde el diseño del procesador hasta la fase de aplicación, sea transparente y se pueda revisar; señala que, a fin de recuperar la competitividad en el sector estratégico de los servicios informáticos, es necesario que las instituciones de la UE, los Estados miembros, las instituciones de investigación, la industria y la sociedad civil alcancen un nuevo acuerdo digital y realicen esfuerzos conjuntos a gran escala; 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; insta por tanto a la Comisión a revisar las prácticas vigentes en materia de contratación pública por lo que se refiere al procesamiento de datos, a fin de estudiar la posibilidad de limitar los procedimientos de licitación a las empresas certificadas, y posiblemente a empresas de la UE, cuando entren en juego intereses vitales o de seguridad;
92. Condena firmemente el que servicios de inteligencia extranjeros hayan intentado rebajar los estándares de seguridad informática e instalar puertas traseras en un amplio espectro de sistemas informáticos; pide a la Comisión que presente proyectos de legislación que prohíban el empleo de puertas traseras por parte de las fuerzas o cuerpos de seguridad; recomienda, en consecuencia, que se emplee software de código abierto en todos los entornos en los que la seguridad informática sea motivo de preocupación;
93. Hace un llamamiento a los Estados miembros, a la Comisión, al Consejo y al Consejo

Europeo para que apoyen plenamente, asimismo mediante financiación en materia de investigación y desarrollo, el desarrollo de una capacidad europea innovadora y tecnológica en materia de herramientas, empresas y proveedores informáticos (hardware, software, servicios y redes), también a efectos de ciberseguridad y capacidades criptográficas y de cifrado; pide a todas las instituciones competentes de la UE y a los Estados miembros que inviertan en tecnologías locales e independientes de la UE y que desarrollen e incrementen en gran medida sus capacidades de detección;

94. Pide a la Comisión, a los organismos de normalización y a ENISA que desarrollen, antes de diciembre de 2014, estándares y directrices mínimos en materia de seguridad e intimidad para los sistemas, redes y servicios informáticos, incluidos los servicios de computación en nube, con el fin de proteger mejor los datos personales de los ciudadanos de la UE y la integridad de todos los sistemas informáticos; cree que dichos estándares podrían convertirse en el patrón para unos nuevos estándares mundiales y deberían fijarse en un proceso abierto y democrático, en lugar de estar dirigidos por un solo país, entidad o empresa multinacional; opina que, aunque hay que tener en cuenta los legítimos motivos de preocupación en el ámbito policial y de la inteligencia a fin de respaldar la lucha contra el terrorismo, no deberían conllevar un debilitamiento general de la fiabilidad de todos los sistemas informáticos; manifiesta su apoyo a las recientes decisiones del Grupo Especial sobre Ingeniería de Internet (IETF) de incluir a los gobiernos en el modelo de amenazas para la seguridad en línea;
95. Señala que los reguladores de las telecomunicaciones a escala nacional y de la UE, y en algunos casos también las empresas de telecomunicaciones, han descuidado claramente la seguridad informática de sus usuarios y clientes; pide a la Comisión que emplee todos los poderes de que disponga 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 e integral de las comunicaciones;
96. Respalda la estrategia cibernética de la UE, pero considera que no abarca todas las amenazas posibles y debería ampliarse para que incluya comportamientos estatales maliciosos; hace hincapié en la necesidad de que los sistemas informáticos dispongan de una seguridad y una resiliencia informáticas más sólidas;
97. Pide a la Comisión que presente, a más tardar en 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 (incluidos sistemas informáticos, equipos, servicios, computación en nube, cifrado y anonimización) y para proteger la infraestructura informática crítica (también en términos de propiedad y vulnerabilidad);
98. Pide a la Comisión, en el marco del siguiente programa de trabajo del programa Horizonte 2020, que destine más recursos al fomento de la investigación, el desarrollo, la innovación y la formación europeos en el ámbito de las tecnologías de la información, y, en particular, en tecnologías e infraestructuras de protección de la intimidad, criptología, computación segura, las mejores posibles soluciones de seguridad, incluida

seguridad de código abierto, y otros servicios de la sociedad de la información, así como que promueva el mercado interior de software y hardware europeos, y medios e infraestructuras de comunicación cifrados, también mediante el desarrollo de una estrategia industrial para la industria informática de la UE exhaustiva; opina que las pequeñas y medianas empresas desempeñan una función especial en la investigación; hace hincapié en que no debe concederse ningún tipo de financiación de la UE a proyectos que tengan como único objetivo desarrollar instrumentos para acceder de forma ilegal a sistemas informáticos;

99. Solicita a la Comisión que planifique las responsabilidades actuales y examine, para diciembre de 2014 a más tardar, la necesidad de un mandato más amplio, una mejor coordinación y/o recursos y capacidades técnicas adicionales para ENISA, el Centro de Ciberdelincuencia de Europol y otros centros de la Unión de conocimientos especializados, CERT-UE y el SEPD, con el fin de que puedan desempeñar un papel clave en la seguridad de los sistemas europeos de comunicación, sean más eficaces en la prevención e investigación de delitos informáticos de gran calado 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; pide, en particular, a la Comisión que estudie la posibilidad de reforzar el papel de ENISA en defensa de los sistemas internos de las instituciones de la UE y establezca un equipo de respuesta a emergencias informáticas (CERT) para la UE y sus Estados miembros en el marco de la estructura de ENISA;
100. Pide a la Comisión que evalúe la necesidad de una Academia de Tecnologías de la Información de la UE que reúna a los mejores expertos europeos e internacionales independientes de todos los campos relacionados y se encargue de proporcionar a todas las instituciones y organismos pertinentes de la UE asesoramiento científico en materia de tecnologías de la información, incluidas estrategias relacionadas con la seguridad;
101. Hace un llamamiento a los servicios competentes de la Secretaría General del Parlamento Europeo para que, bajo la responsabilidad del presidente del Parlamento, lleve a cabo, a más tardar en junio de 2015, presentándose un informe intermedio a más tardar en diciembre de 2014, una profunda revisión y evaluación de la fiabilidad de la seguridad informática del Parlamento centrada en: medios presupuestarios, recursos de personal, capacidades técnicas, organización interna y todos los elementos oportunos para conseguir un elevado nivel de seguridad de los sistemas informáticos del Parlamento; cree que dicha evaluación debería aportar información, análisis y recomendaciones sobre lo siguiente:
- 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 la salvaguardia de sus credenciales frente a terceros países o a cualquier tipo de intereses creados;
 - la inclusión en los procedimientos de licitación para nuevos sistemas informáticos de requisitos de mejores prácticas informáticas específicas en materia de seguridad e intimidad, incluida la posibilidad de un requisito de software de código abierto como condición de compra o el requisito de que empresas europeas de confianza formen parte de la licitación en el caso de que afecte a áreas sensibles relacionadas con la seguridad;

- la lista de empresas que trabajan con el Parlamento en los campos de la informática y las telecomunicaciones, teniendo en cuenta cualquier información que haya salido a la luz sobre su cooperación con agencias de inteligencia (como las revelaciones acerca de los contratos de la Agencia Nacional de Seguridad con empresas como RSA, cuyos productos emplea el Parlamento Europeo para supuestamente proteger el acceso remoto a sus datos por parte de sus diputados y su personal), incluida la viabilidad de que otras empresas, preferiblemente europeas, puedan prestar los mismos servicios;
- la fiabilidad y resistencia del software y, en especial, el software comercial genérico, utilizado por las instituciones de la UE en sus sistemas informáticos en lo que respecta a la intromisión y penetración por las fuerzas del orden y las autoridades de inteligencia de la UE o de terceros países, teniendo asimismo en cuenta las normas internacionales pertinentes, las mejores prácticas en cuanto a principios de gestión de riesgos de seguridad y el respeto de las normas en materia de seguridad de las redes y de la información de la UE por lo que respecta a las violaciones de la seguridad;
- el uso de más sistemas de código abierto;
- los pasos y medidas que habrá que seguir para hacer frente al aumento del uso de herramientas móviles (como teléfonos inteligentes 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 y de los sistemas informáticos utilizados en él;
- el uso y la ubicación de los servidores y centros informáticos para los sistemas informáticos del Parlamento 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 servicios de computación y almacenamiento en nube por el Parlamento, incluida la índole de los datos almacenados en la nube, cómo se protege el contenido y el acceso al mismo y dónde se ubica la nube, aclarando cuál es el marco jurídico de protección e inteligencia de datos aplicable y evaluando las posibilidades de emplear únicamente servidores en nube que estén basados en territorio de la UE;
- un plan que permita el uso de más tecnologías criptográficas, especialmente cifrado autenticado 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 firmas electrónicas en el correo electrónico;
- un plan para emplear un estándar de cifrado predeterminado, como GNU Privacy Guard, para los correos electrónicos que permitiese al mismo tiempo el uso de

firmas digitales;

- la posibilidad de establecer un servicio seguro de mensajería instantánea dentro del Parlamento que garantice una comunicación segura y en el que el servidor solo vea contenido cifrado;
102. Hace un llamamiento a todas las instituciones y agencias de la UE para que lleven a cabo un ejercicio similar en cooperación con ENISA, Europol y los CERT a más tardar en junio de 2015, presentándose un informe intermedio a más tardar en diciembre de 2014, en especial al Consejo Europeo, el Consejo, el Servicio Europeo 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;
 103. Destaca que, en lo que concierne a la acción exterior de la UE, deberían llevarse a cabo evaluaciones de las necesidades presupuestarias relacionadas y, en el caso del Servicio Europeo de Acción Exterior (SEAE), deberían tomarse las primeras medidas sin demora, y que deben destinarse los fondos necesarios en el proyecto de presupuesto para 2015;
 104. 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, como EU-ESTA, deberían desarrollarse y operarse de tal forma que se garantice que los datos no se pongan en peligro como resultado de las solicitudes presentadas por autoridades de terceros países; pide a eu-LISA que informe al Parlamento sobre la fiabilidad de los sistemas utilizados antes de finales de 2014;
 105. Pide a la Comisión y al SEAE que emprendan acciones a nivel internacional, especialmente con las Naciones Unidas, y que, en colaboración con socios interesados, pongan en práctica una estrategia de la UE 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, al mismo tiempo que se dificulta el control o la censura estatal y la «balcanización» y fragmentación de internet;
 106. Pide a la UE que tome la iniciativa a la hora de rediseñar la arquitectura y la gobernanza de internet a fin de hacer frente a los riesgos vinculados con el almacenamiento y los flujos de datos, procurando conseguir una mayor transparencia y minimización de los datos y un menor almacenamiento masivo centralizado de los datos en bruto, así como una reorganización del tráfico de internet o un cifrado integral pleno de todo el tráfico de internet, a fin de evitar los riesgos que existen actualmente y que se derivan de una redirección innecesaria del tráfico a través del territorio de países que no cumplen los estándares básicos en materia de derechos fundamentales, protección de datos e intimidad;
 107. Pide la promoción de:
 - motores de búsqueda y redes sociales de la UE como paso útil para avanzar hacia la independencia informática de la UE;

- proveedores europeos de servicios informáticos;
 - el cifrado de comunicaciones en general, incluida la comunicación por correo electrónico y SMS;
 - elementos informáticos clave europeos, como soluciones para sistemas operativos cliente/servidor, el empleo de normas de código abierto o el desarrollo de elementos europeos de acoplamiento de red (por ejemplo, combinadores de redes);
108. Pide a la Comisión que presente una propuesta jurídica para un sistema de organización del tráfico de la UE, incluido el tratamiento del registro de detalle de llamada a escala de la UE, que constituya una subestructura de la actual red de internet y no rebase las fronteras de la UE; toma nota de que todos los datos de tráfico y del registro de detalle de llamada deben tratarse con arreglo al marco jurídico de la UE;
109. Hace un llamamiento a los Estados miembros, en colaboración con ENISA, el Centro de Ciberdelincuencia de Europol, los CERT y las autoridades de protección de datos y las unidades de ciberdelincuencia nacionales para que desarrollen una cultura de seguridad y lancen 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, incluido a través del cifrado y una computación en nube segura, haciendo pleno uso de la plataforma de información de interés público establecida en la Directiva de servicio universal;
110. Pide a la Comisión que, antes de diciembre de 2014, presente proyectos legislativos destinados a alentar a los fabricantes de software y hardware para que introduzcan más características de seguridad e intimidad desde el diseño o por defecto en sus productos, también introduciendo desincentivos a la recogida indebida y desproporcionada de datos personales masivos y haciendo a los fabricantes legalmente responsables por la omisión de parchear vulnerabilidades conocidas, software defectuoso o inseguro o la instalación de puertas traseras secretas que permitan el acceso y el tratamiento no autorizados de los datos; pide en este sentido a la Comisión que evalúe la posibilidad de establecer un sistema de certificación o validación de hardware informático que incluya procedimientos de ensayo a nivel de la UE a fin de garantizar la integridad y la seguridad de los productos;

Recuperación de la confianza

111. Cree que, aparte de la necesidad de un cambio legislativo, la investigación ha mostrado la necesidad de que los Estados Unidos recuperen la confianza de sus socios de la UE, ya que lo que está en juego son esencialmente las actividades de las agencias de inteligencia de los Estados Unidos;
112. 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 espíandolos;

- el respeto de los derechos fundamentales, la democracia y el Estado de Derecho, así como la credibilidad de las salvaguardas y el control democráticos, jurídicos y parlamentarios en una sociedad digital;

Entre la UE y Estados Unidos

113. 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;
114. Cree que la vigilancia masiva de los ciudadanos y el espionaje de los líderes políticos por parte de los Estados Unidos ha causado graves 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;
115. Reconoce, a la luz de los retos mundiales a los que se enfrentan la UE y los Estados Unidos, que la asociación transatlántica tiene que fortalecerse más, y que es vital que continúe la cooperación transatlántica en la lucha antiterrorista sobre una nueva base de confianza que se fundamente en un verdadero respeto común del Estado de Derecho y en el rechazo de todas las prácticas indiscriminadas de vigilancia masiva; insiste por tanto 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;
116. Está preparado para entablar un 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— en los tribunales de Estados Unidos se garanticen el derecho a la intimidad y otros derechos de los ciudadanos y residentes de la UE u otras personas protegidas por el Derecho de la UE y unos derechos de información y una protección de la intimidad equivalentes a través de, por ejemplo, una revisión de la Ley sobre la vida privada y la Ley de Intimidad de las Comunicaciones Electrónicas, y la ratificación del primer protocolo opcional al Pacto internacional de derechos civiles y políticos (PIDCP), de modo que deje de perpetuarse la actual discriminación;
117. Insiste en que deben emprenderse reformas necesarias y deben ofrecerse garantías efectivas a los europeos para que el uso de la vigilancia y el tratamiento de datos con fines de inteligencia exterior sean proporcionados y estén limitados por condiciones especificadas claramente y vinculados a sospechas razonables y causas probables de actividades terroristas; destaca que este fin debe estar sujeto a un control judicial transparente;
118. Considera que nuestros socios estadounidenses deben enviar señales políticas para demostrar que los Estados Unidos distinguen entre aliados y enemigos;
119. Insta a la Comisión y al Gobierno de los Estados Unidos a abordar, en el contexto de las negociaciones en curso sobre un acuerdo marco entre la UE y Estados Unidos sobre el intercambio de datos con fines policiales, los derechos de información y recurso 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 UE-Estados Unidos del 18 de noviembre de 2013, antes del verano de 2014;

120. Alienta a los Estados Unidos a que se adhieran al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), al igual que se adhirieron al Convenio sobre la Ciberdelincuencia de 2001, reforzando de ese modo la base jurídica compartida por los aliados transatlánticos;
121. Hace un llamamiento a las instituciones de la UE para que exploren las posibilidades de establecer un código de conducta con los Estados Unidos que pudiera garantizar que no se lleven a cabo actividades de espionaje estadounidenses contra instituciones ni instalaciones de la UE;

Dentro de la Unión Europea

122. Está asimismo convencido de que la implicación y actividades de algunos Estados miembros de la UE ha provocado una pérdida de confianza, incluso entre Estados miembros y entre los ciudadanos de la UE y sus autoridades nacionales; opina que únicamente mediante una total claridad en cuanto a los fines y medios de la vigilancia, un debate público y, en última instancia, una revisión de la legislación, incluido el fin de las actividades de vigilancia masiva y el refuerzo de los sistemas de control judicial y parlamentario, se conseguirá restablecer la confianza perdida; reitera las dificultades que implica el desarrollo unas políticas integrales de seguridad de la UE mientras estén en marcha este tipo de actividades de vigilancia masiva, y hace hincapié en que el principio de cooperación leal de la UE exige que los Estados miembros se abstengan de llevar a cabo actividades de inteligencia en el territorio de otros Estados miembros;
123. Señala que algunos Estados miembros están llevando a cabo intercambios bilaterales con las autoridades de los Estados Unidos sobre las acusaciones de espionaje, y que algunos de ellos han pactado (Reino Unido) o prevén pactar (Alemania, Francia) acuerdos antiespionaje; subraya que dichos Estados miembros tienen que respetar plenamente los intereses y el marco legislativo de la UE en su conjunto; considera que dichos acuerdos bilaterales son contraproducentes e irrelevantes, dada la necesidad de encontrar un planteamiento europeo para este problema; pide al Consejo que informe al Parlamento sobre los avances por parte de los Estados miembros para un acuerdo antiespionaje mutuo a escala de la UE;
124. Considera que dichos acuerdos no deben vulnerar los Tratados de la Unión, especialmente el principio de cooperación leal (con arreglo al apartado 3 del artículo 4 del TUE), 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; decide revisar este tipo de acuerdos para determinar su compatibilidad con el Derecho europeo, y se reserva el derecho de activar los procedimientos aplicables 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;
125. Pide a los Estados miembros que hagan todo lo posible para garantizar una mejor cooperación con el fin de ofrecer salvaguardias contra el espionaje, en cooperación con las agencias y los organismos pertinentes de la UE, para la protección de los ciudadanos

y las instituciones de la UE, las empresas europeas, la industria y la infraestructura y redes informáticas de la UE, así como la investigación europea; considera que la participación activa de las partes interesadas de la UE es una condición previa para un intercambio eficaz de información; señala que las amenazas a la seguridad se han vuelto más internacionales, difusas y complejas, lo que requiere una cooperación reforzada europea; considera que este desarrollo debería reflejarse mejor en los Tratados, por lo que pide una revisión de los Tratados con el fin de reforzar la noción de cooperación leal entre los Estados miembros y la Unión en lo que respecta al objetivo de lograr un espacio de seguridad y de evitar el espionaje mutuo entre los Estados miembros dentro de la Unión;

126. Opina que resulta absolutamente necesario contar con estructuras de comunicación a prueba de interceptaciones (correo electrónico y telecomunicaciones, incluida la telefonía fija y móvil) y con salas de reunión a prueba de interceptaciones en todas las instituciones y delegaciones de la UE pertinentes; pide, por tanto, el establecimiento de un sistema de correo electrónico interno y cifrado para la UE;
127. Pide al Consejo ya la Comisión que concedan sin más demora su aprobación a la propuesta adoptada por el Parlamento Europeo, de 23 de mayo de 2012, sobre el Reglamento del Parlamento Europeo relativo a las modalidades de ejercicio del derecho de investigación del Parlamento Europeo y por el que se deroga la Decisión 95/167/CE, Euratom, CECA del Parlamento Europeo, del Consejo y de la Comisión, presentada sobre la base del artículo 226 del TFUE; pide una revisión del Tratado con el fin de ampliar este tipo de poderes de investigación para que cubran, sin restricciones ni excepciones, todos los ámbitos de competencias o actividades de la Unión, y de incluir la posibilidad de interrogar bajo juramento;

Aspectos internacionales

128. Hace un llamamiento a la Comisión para que presente, a más tardar en enero de 2015, una estrategia de la UE para una gobernanza democrática de Internet;
129. 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 (PIDCP), 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 Comité de Derechos Humanos sobre el Pacto para crear estándares aplicables en todo el mundo de protección de datos y de la intimidad con arreglo al Estado de Derecho; pide a los Estados miembros que incluyan en este ejercicio un llamamiento en favor de una agencia internacional de las Naciones Unidas encargada especialmente de controlar la aparición de herramientas de vigilancia y de regular e investigar su uso; solicita a la Alta Representante / Vicepresidenta de la Comisión y al Servicio Europeo de Acción Exterior que adopten una posición más activa;
130. Hace un llamamiento a los Estados miembros para que desarrollen una estrategia sólida y coherente dentro de las Naciones Unidas, apoyando en especial la resolución sobre «el derecho a la intimidad en la era digital», presentada por Brasil y Alemania, tal y como la adoptó el Tercer Comité de la Asamblea General de las Naciones Unidas (Comité de Derechos Humanos) el 27 de noviembre de 2013, así como tomando medidas en defensa

del derecho fundamental a la intimidad y a la protección de los datos a escala internacional, pero evitando no obstante cualquier facilitación del control o la censura estatales o la fragmentación de internet, incluida una iniciativa de cara a un tratado internacional por el que se prohíban las actividades de vigilancia masiva y una agencia para su control;

Plan de prioridades: Habeas corpus digital europeo – proteger los derechos fundamentales en una era digital

131. Decide presentar a los ciudadanos, instituciones y Estados miembros de la UE las recomendaciones antes citadas como un plan de prioridades para la próxima legislatura; pide a la Comisión y a las demás instituciones, órganos y organismos de la UE a que se hace referencia en la presente Resolución que actúen con arreglo a las recomendaciones y solicitudes de la presente Resolución, de conformidad con el artículo 265 del TFUE;
132. Decide presentar un «Habeas corpus digital europeo – proteger los derechos fundamentales en una era digital» con las ocho acciones siguientes, cuya aplicación supervisará:
 - Acción 1: Adopción del paquete de protección de datos en 2014;
 - Acción 2: Conclusión del acuerdo marco entre la UE y los Estados Unidos que garantice el derecho fundamental de los ciudadanos a la intimidad y a la protección de datos y los mecanismos de recurso adecuados para los ciudadanos de la UE, incluso en caso de que se produzcan envíos de datos de la UE a los Estados Unidos con fines coercitivos;
 - Acción 3: Suspensión del 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 llevarse a cabo de conformidad con los máximos estándares de la UE;
 - Acción 4: Suspensión del acuerdo TFTP hasta que i) se hayan cerrado las negociaciones del acuerdo marco; ii) se haya efectuado una investigación exhaustiva sobre la base de un análisis de la UE y se hayan abordado debidamente todos los problemas planteados por el Parlamento en su Resolución de 23 de octubre de 2013;
 - Acción 5: Evaluación de todo acuerdo, mecanismo o intercambio con terceros países que implique datos personales a fin de garantizar que no se infringe el derecho a la intimidad y a la protección de los datos personales debido a las actividades de vigilancia, y adopción de las medidas de seguimiento necesarias;
 - Acción 6: Protección del Estado de Derecho y los derechos fundamentales de los ciudadanos de la UE (también de las amenazas a la libertad de prensa), el derecho del público a recibir información objetiva y acogerse al secreto profesional (incluidas las relaciones entre abogados y clientes), así como la garantía de una mejor protección de los denunciantes de irregularidades;
 - Acción 7: Desarrollo de una estrategia europea para una mayor independencia

informática (un «nuevo acuerdo digital» que incluya la asignación de recursos adecuados a nivel nacional y de la UE), a fin de potenciar la industria informática y permitir que las empresas europeas exploten la ventaja competitiva de la UE en términos de intimidad;

- Acción 8: Desarrollo de la UE como actor de referencia para una gobernanza democrática y neutral de internet;

133. Hace un llamamiento a las instituciones y Estados miembros de la UE para que promuevan el «Habeas corpus digital europeo – proteger los derechos fundamentales en una era digital»; se compromete a actuar como el defensor de los derechos de los ciudadanos de la UE, con el siguiente plan de seguimiento de la puesta en práctica:

- Abril de 2014 - marzo de 2015: un grupo de seguimiento basado en el equipo de investigación de la Comisión LIBE responsable de hacer un seguimiento de cualquier revelación nueva 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 los envíos de datos y los recursos judiciales dentro de la comisión competente;
- Primavera de 2014: una petición formal al Consejo Europeo para que incluya el «Habeas corpus digital europeo – proteger los derechos fundamentales en una era digital» en las directrices que habrán de adoptarse con arreglo al artículo 68 del TFUE;
- Otoño de 2014: un compromiso de que el «Habeas corpus digital europeo – proteger los derechos fundamentales en una era digital» y las recomendaciones relacionadas serán criterios clave para la aprobación de la siguiente Comisión;
- 2014: una conferencia que reúna a expertos europeos de alto nivel en los diversos ámbitos que contribuyen a 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;
- 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 otros terceros países comprometidos, incluido el brasileño;
- 2014-2015: una conferencia con los organismos de control de los servicios de inteligencia de los parlamentos nacionales europeos;

o

o o

134. 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 Federativa de Brasil y al Secretario General de las Naciones Unidas.

135. Encarga a su Comisión de Libertades Civiles, Justicia y Asuntos de Interior que aborde esta cuestión ante el Pleno un año después de la aprobación de la presente Resolución; considera esencial evaluar el grado de seguimiento de las recomendaciones aprobadas por el Parlamento y analizar, en su caso, las razones por las que no se hayan seguido.