Martes, 8 de septiembre de 2015

P8_TA(2015)0288

Derechos humanos y tecnología en terceros países

Resolución del Parlamento Europeo, de 8 de septiembre de 2015, sobre «Derechos humanos y tecnología: el impacto de los sistemas de intrusión y vigilancia en los derechos humanos en terceros países» (2014/2232(INI))

(2017/C 316/03)

El Parlamento Europeo,

— Vistos la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, en particular su artículo 19,

— Visto el Marco estratégico sobre derechos humanos y democracia de la Unión Europea, adoptado por el Consejo el 25 de junio de 2012 ([1]),

— Vistas las orientaciones en materia de derechos humanos de la UE sobre la libertad de expresión en línea o no, adoptadas por el Consejo de Asuntos Exteriores el 12 de mayo de 2014 ([2]),

— Vista la Guía sobre la aplicación en el sector de las TIC de los Principios Rectores de las Naciones Unidas sobre las empresas y los derechos humanos, publicada por la Comisión en junio de 2013,

— Vistos el informe de la Organización para la Seguridad y la Cooperación en Europa (OSCE), de 15 de diciembre de 2011, titulado «La libertad de expresión en Internet» ([3]) y el informe periódico del Representante Especial de la OSCE para la Libertad de los Medios de Comunicación al Consejo Permanente de la OSCE de 27 de noviembre de 2014 ([4]),

— Visto el informe del Relator Especial de las Naciones Unidas sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, de 23 de septiembre de 2014 (A/69/397) ([5]),

— Visto el informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos de 30 de junio de 2014 titulado «El derecho a la privacidad en la era digital» ([6]),

— Visto el informe del Relator Especial de las Naciones Unidas, de 17 de abril de 2013, sobre el derecho a la libertad de opinión y expresión (A/HRC/23/40), en el que se analizan las consecuencias de la vigilancia de las comunicaciones por los Estados en el ejercicio de los derechos humanos a la intimidad y a la libertad de opinión y expresión,

— Visto el informe de la Comisión de Asuntos Jurídicos y Derechos Humanos de la Asamblea Parlamentaria del Consejo de Europa, de 26 de enero de 2015, sobre vigilancia masiva ([7]),

— Vista su Resolución, 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 ([8]),

---

([1]) http://eeas.europa.eu/delegations/un_geneva/press_corner/focus/events/2012/20120625_en.htm
([2]) http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf
([3]) http://www.osce.org/fom/80723?download=true.
([4]) http://www.osce.org/fom/127656?download=true .
([5]) http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement.
([6]) http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_sp.doc.
([7]) http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10-b7a2.
([8]) Textos Aprobados, P7_TA(2014)0230.

— Visto el informe del Representante Especial del Secretario General de las Naciones Unidas para la cuestión de los derechos humanos y las empresas transnacionales y otras empresas comerciales, de 21 de marzo de 2011, titulado «Principios rectores sobre las empresas y los derechos humanos: Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar"» ([1]),

— Vistos las directrices de la OCDE para las empresas multinacionales ([2]) y el informe anual de 2014 sobre las directrices de la OCDE para las empresas multinacionales ([3]),

— Visto el Informe anual de la Corporación de Asignación de Nombres y Números de Internet de 2013 ([4]),

— Vista la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 12 de febrero de 2014, titulada «La política y la gobernanza de Internet — El papel de Europa en la configuración de la gobernanza de Internet» ([5]),

— Vista la Declaración multisectorial de NETmundial, adoptada el 24 de abril de 2014 ([6]),

— Visto el resumen de la Presidencia del noveno Foro para la Gobernanza de Internet, celebrado en Estambul del 2 al 5 de septiembre de 2014,

— Vistas las medidas restrictivas en vigor de la Unión Europea, que en algunos casos comprenden embargos de equipos de telecomunicaciones, tecnologías de la información y la comunicación (TIC) y herramientas de seguimiento,

— Visto el Reglamento (UE) nº 599/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, que modifica el Reglamento (CE) nº 428/2009 del Consejo por el que se establece un régimen comunitario de control de las exportaciones, la transferencia, el corretaje y el tránsito de productos de doble uso ([7]),

— Vista la Declaración conjunta del Parlamento Europeo, el Consejo y la Comisión sobre la revisión del sistema de control de las exportaciones de doble uso, de 16 de abril de 2014 ([8]),

— Vistas las decisiones adoptadas en la 19ª Sesión Plenaria del Arreglo de Wassenaar sobre control de exportaciones de armas convencionales y bienes y tecnología de doble uso, celebrada en Viena los días 3 y 4 de diciembre de 2013,

— Vista la Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 24 de abril de 2014, titulada «Revisión de la política de control de las exportaciones: garantizar la seguridad y la competitividad en un mundo cambiante» ([9]),

— Vistas las Conclusiones del Consejo de 21 de noviembre de 2014 sobre la revisión de la política de control de las exportaciones,

— Vista su Resolución, de 11 de diciembre de 2012, sobre una Estrategia de libertad digital en la política exterior de la UE ([10]),

---

([1]) http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf
([2]) http://www.oecd.org/daf/inv/mne/48004323.pdf
([3]) http://www.oecd-ilibrary.org/docserver/download/2014091e.pdf?expires=1423160236&id=id&accname=ocid194994&checksum=D1FC664FBCEA28FC856AE63932715B3C
([4]) https://www.icann.org/en/system/files/files/annual-report-2013-en.pdf
([5]) COM(2014)0072.
([6]) http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf
([7]) DO L 173 de 12.6.2014, p. 79.
([8]) DO L 173 de 12.6.2014, p. 82.
([9]) COM(2014)0244.
([10]) Textos Aprobados, P7_TA(2012)0470.

Martes, 8 de septiembre de 2015

— Vista su Resolución, de 13 de junio de 2013, sobre la libertad de prensa y de los medios de comunicación en el mundo ([1]),

— Vistas sus Resoluciones sobre casos urgentes de violaciones de los derechos humanos, la democracia y el Estado de Derecho, en las que se expresa la preocupación por las libertades digitales,

— Vista su Resolución, de 12 de marzo de 2015, sobre las prioridades de la UE para el Consejo de Derechos Humanos de las Naciones Unidas en 2015 ([2]),

— Vista su Resolución, de 11 de febrero de 2015, sobre la renovación del mandato del Foro para la Gobernanza de Internet, ([3])

— Vista su Resolución de 12 de marzo de 2015 sobre el Informe anual sobre los derechos humanos y la democracia en el mundo (2013) y la política de la Unión Europea al respecto ([4]),

— Vista la declaración por escrito de Edward Snowden dirigida a la Comisión LIBE, de marzo de 2014 ([5]),

— Visto el Convenio Europeo de Derechos Humanos y las negociaciones en curso sobre la adhesión de la UE a este,

— Vista la Carta de los Derechos Fundamentales de la Unión Europea,

— Visto el artículo 52 de su Reglamento,

— Visto el informe de la Comisión de Asuntos Exteriores (A8-0178/2015),

A. Considerando que los avances tecnológicos y el acceso no censurado a Internet desempeñan un papel cada vez más importante a la hora de permitir y garantizar la aplicación y el pleno respeto de los derechos humanos y las libertades fundamentales y han tenido un efecto positivo, al ampliar el ámbito de la libertad de expresión, el acceso a la información, el derecho a la privacidad y la libertad de reunión y asociación en todo el mundo;

B. Considerando que los sistemas tecnológicos se pueden utilizar indebidamente como instrumentos para la vulneración de los derechos humanos, a través de la censura, la vigilancia, el acceso no autorizado a dispositivos, la interferencia intencionada, y el seguimiento y rastreo de la información y los ciudadanos;

C. Considerando que tales actividades las llevan a cabo agentes públicos y privados, incluidos gobiernos, fuerzas y cuerpos de seguridad, así como organizaciones delictivas y redes terroristas con el fin de vulnerar los derechos humanos;

D. Considerando que el contexto en el que se diseñan y utilizan las TIC determina, en gran medida, el efecto que pueden ejercer como factor de impulso —o conculcación— de los derechos humanos; que la tecnología de la información, sobre todo el *software*, no suele ser de uso único, sino de doble uso, por lo que se refiere al potencial de vulneración de los derechos humanos, mientras que el *software* constituye asimismo una forma de expresión;

E. Considerando que las TIC han sido instrumentos fundamentales a la hora de ayudar a las personas en la organización de movimientos sociales y protestas en diversos países, sobre todo en aquellos con regímenes autoritarios;

([1]) Textos Aprobados, P7_TA(2013)0274.
([2]) Textos Aprobados, P8_TA(2015)0079.
([3]) Textos Aprobados, P8_TA(2015)0033.
([4]) Textos Aprobados, P8_TA(2015)0076.
([5]) http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

F. Considerando que la evaluación de las implicaciones para los derechos humanos del contexto en que se utilicen las tecnologías queda determinada por la rigurosidad con que los marcos jurídicos nacionales y regionales regulan la utilización de las tecnologías y la capacidad de los entes políticos y judiciales para supervisar dicha utilización;

G. Considerando que, en el ámbito digital, los agentes privados desempeñan un papel cada vez más significativo en todas las esferas de las actividades sociales, pero aún no se han tomado medidas de salvaguardia que les impidan imponer restricciones excesivas a los derechos y libertades fundamentales; que, en consecuencia, los agentes privados desempeñan un papel más activo en la evaluación de la legalidad del contenido y en el desarrollo de sistemas de ciberseguridad y de vigilancia, que pueden menoscabar los derechos humanos a escala mundial;

H. Considerando que Internet representa una revolución en las posibilidades que ofrece en materia de intercambio de datos, informaciones y conocimientos de todo tipo;

I. Considerando que el cifrado es un importante método que ayuda a dotar de seguridad a las comunicaciones y a las personas que las utilizan;

J. Considerando que la gobernanza de Internet se ha beneficiado de un modelo de toma de decisiones de múltiples interlocutores, un proceso que garantiza la participación significativa, incluyente y responsable de todas las partes interesadas, incluidos los gobiernos, la sociedad civil, las comunidades técnicas y académicas, el sector privado y los usuarios;

K. Considerando que las agencias de inteligencia han socavado de forma sistemática los protocolos y productos de cifrado para poder interceptar comunicaciones y datos; que la Agencia Nacional de Seguridad de los Estados Unidos ha recopilado cantidades ingentes de los llamados «ataques de día cero», esto es, vulnerabilidades de seguridad informática todavía desconocidas para el público o el vendedor del producto, que tales actividades socavan los esfuerzos mundiales para mejorar la seguridad informática;

L. Considerando que servicios de inteligencia con sede en la UE han realizado actividades que vulneran los derechos humanos;

M. Considerando que, habida cuenta de los rápidos avances tecnológicos que se están produciendo, los controles y garantías judiciales y democráticos están poco desarrollados;

N. Considerando que la (ciber)seguridad y las medidas de lucha contra el terrorismo en las que intervienen las TIC, así como la vigilancia de Internet, pueden menoscabar de manera significativa los derechos humanos y libertades fundamentales de personas de todo el mundo, incluidos los ciudadanos de la UE cuando residen o viajan fuera de su país, sobre todo en ausencia de un fundamento jurídico basado en los principios de necesidad, proporcionalidad y una supervisión democrática y judicial;

O. Considerando que los filtros de Internet y la vigilancia de las comunicaciones socavan la capacidad de los defensores de los derechos humanos de sacar partido de Internet y comunicar información delicada, y que contravienen varios artículos de la Declaración Universal de Derechos Humanos (DUDH) que garantizan los derechos de cada persona a la intimidad y a la libertad de expresión;

P. Considerando que tanto la seguridad digital como la libertad digital son elementos esenciales y no pueden sustituirse entre sí, sino que han de reforzarse mutuamente;

Q. Considerando que, por lo que se refiere a las libertades digitales, la Unión Europea solo podrá predicar con el ejemplo cuando estas libertades se encuentren salvaguardadas en la propia UE; que resulta fundamental, por tanto, la adopción del paquete de medidas de la UE sobre protección de datos;

R. Considerando que están en juego amplios intereses de la sociedad, como la protección de los derechos fundamentales, que no deben dejarse exclusivamente en manos del mercado, sino que requieren una regulación;

S. Considerando que el respeto de los derechos fundamentales y del Estado de Derecho y el control parlamentario efectivo de los servicios de inteligencia que utilizan tecnología de vigilancia digital constituyen importantes elementos de cooperación internacional;

T. Considerando que las empresas con sede en la UE cuentan con una importante participación en el mercado mundial de las TIC, sobre todo en lo que respecta a la exportación de tecnología de vigilancia, rastreo, intrusión y seguimiento;

U. Considerando que la introducción de controles de las exportaciones no debería socavar la investigación legítima de cuestiones de seguridad informática ni el desarrollo sin dolo de herramientas de seguridad informática;

1. Es consciente de que los derechos humanos y las libertades fundamentales son universales y deben defenderse en todo el mundo y en todos sus ámbitos de expresión; hace hincapié en que la vigilancia de las comunicaciones afecta, como tal, a los derechos a la intimidad y a la libertad de expresión, a menos que se lleve a cabo dentro de un marco jurídico adecuado;

2. Solicita a la Comisión que garantice la coherencia entre las acciones externas de la UE y sus políticas internas relacionadas con las TIC;

3. Considera que la complicidad activa de determinados Estados miembros de la UE en la vigilancia masiva de los ciudadanos y el espionaje de los dirigentes políticos por parte de la Agencia Nacional de Seguridad, tal como reveló Edward Snowden, ha socavado en gran medida la credibilidad de la política de la UE en materia de derechos humanos y ha minado la confianza mundial en las ventajas de las TIC;

4. Recuerda a los Estados miembros y a las agencias de la UE en cuestión, incluidas Europol y Eurojust, las obligaciones que han contraído en virtud de la Carta de los Derechos Fundamentales de la Unión Europea, y a la hora de respetar el Derecho internacional en materia de derechos humanos, así como los objetivos de política exterior de la UE, de no compartir datos de inteligencia que puedan dar lugar a violaciones de los derechos humanos en un tercer país ni utilizar información obtenida mediante violaciones de los derechos humanos, como la vigilancia ilícita, fuera de la UE;

5. Subraya que la repercusión de las tecnologías en la mejora de los derechos humanos debe incorporarse a todas las políticas y programas de la UE, en su caso, con el fin de fomentar la protección de los derechos humanos y la promoción de la democracia, el Estado de Derecho y la buena gobernanza, así como la resolución pacífica de conflictos;

6. Pide el desarrollo activo y la difusión de las tecnologías que contribuyen a la protección de los derechos humanos, y a facilitar los derechos y las libertades digitales de las personas, así como su seguridad, y que fomentan las mejores prácticas y marcos legislativos adecuados, al tiempo que garantizan la seguridad y la integridad de los datos personales; insta, en particular, a la UE y a sus Estados miembros a que promuevan activamente la utilización global y el desarrollo de normas abiertas y de *software* y tecnologías de cifrado libres, gratuitos y de fuente abierta;

7. Pide a la UE que intensifique su apoyo a los agentes que se dedican a reforzar las normas de seguridad y protección de la intimidad en todos los ámbitos de las TIC, incluidas las normas en materia de *hardware*, *software* y comunicaciones, así como el desarrollo de *hardware* y *software* en marcos de protección de la intimidad desde el diseño;

8. Hace un llamamiento a favor de la creación de un fondo de derechos humanos y tecnología en el marco del Instrumento Europeo para la Democracia y los Derechos Humanos;

9. Insta a la propia UE y, en particular al SEAE, a que cifren sus comunicaciones con los defensores de los derechos humanos a fin de evitar comprometer la seguridad de estas personas y de proteger sus propias comunicaciones con terceros de la vigilancia;

10. Pide a la UE que utilice *software* libre, gratuito y de fuente abierta y que aliente a los demás agentes a hacer lo mismo, ya que este tipo de *software* permite una mayor seguridad y un mayor respeto de los derechos humanos;

11. Atrae la atención sobre la importancia de desarrollar las TIC en las zonas conflictivas para promover actividades de consolidación de la paz con objeto de facilitar una comunicación segura entre las partes intervinientes en la resolución pacífica de conflictos;

12. Pide que se apliquen los requisitos, valores de referencia y procedimientos de presentación de informes oportunos para garantizar que el apoyo técnico y financiero de la UE al desarrollo de nuevas tecnologías en terceros países no se utilice en perjuicio de los derechos humanos;

13. Pide a la Comisión y al Consejo que se comprometan activamente con gobiernos de terceros países y que, con los mecanismos de apoyo y los instrumentos de política europeos, sigan apoyando, formando y habilitando a los defensores de los derechos humanos, a los activistas de la sociedad civil y a los periodistas independientes que utilizan las TIC en sus actividades de forma segura, y que promuevan los derechos fundamentales a la intimidad relacionados, como el acceso ilimitado a los flujos de información en Internet, el derecho a la intimidad y la protección de datos, la libertad de expresión, la libertad de reunión, la libertad de asociación y la libertad de prensa y de publicación en Internet;

14. Atrae la atención sobre la difícil situación de los denunciantes y sus partidarios, incluidos los periodistas, a raíz de las revelaciones de prácticas abusivas de vigilancia en terceros países; considera que estas personas deben ser consideradas defensoras de los derechos humanos y que, como tales, merecen la protección de la UE con arreglo a lo dispuesto en las Directrices de la UE sobre defensores de los derechos humanos; reitera su petición a la Comisión y a los Estados miembros de que estudien detenidamente la posibilidad de conceder a los denunciantes protección internacional contra el enjuiciamiento;

15. Lamenta que las medidas de seguridad, incluidas las medidas antiterroristas, se utilicen cada vez más como pretextos para la conculcación del derecho a la intimidad y para reprimir las actividades legítimas de los defensores de los derechos humanos, periodistas y activistas políticos; reitera su firme convicción de que la seguridad nacional nunca puede constituir una justificación para llevar a cabo programas de vigilancia masiva, no selectivos o secretos; insiste en que dichas medidas deben aplicarse en estricta conformidad con el Estado de Derecho y los derechos humanos, incluido el derecho a la intimidad y a la protección de datos;

16. Pide al SEAE y a la Comisión que promuevan el control democrático de los servicios de seguridad e inteligencia en su diálogo político con terceros países, así como en sus programas de cooperación al desarrollo; insta a la Comisión a que apoye a las organizaciones de la sociedad civil y los órganos legislativos de terceros países que aspiran a reforzar el control, la transparencia y la rendición de cuentas de los servicios de seguridad nacionales; solicita la inclusión de compromisos específicos a este respecto en el futuro Plan de Acción de la UE para los derechos humanos y la democracia;

17. Insta al Consejo y a la Comisión a que fomenten las libertades digitales y el acceso no restringido a Internet en todas las formas de contacto con terceros países, incluidas las negociaciones de adhesión, las negociaciones comerciales, los diálogos sobre derechos humanos y los contactos diplomáticos;

18. Reconoce que Internet se ha convertido en un espacio público y en un mercado para el cual es indispensable que la circulación de la información y el acceso a las TIC sean libres; hace hincapié, por tanto, en la necesidad de promover y proteger al mismo tiempo la libertad digital y el libre comercio;

19. Pide la inclusión de cláusulas en todos los acuerdos con terceros países en las que se aluda explícitamente a la necesidad de promover, garantizar y respetar las libertades digitales, la neutralidad de la red, el acceso no censurado y no restringido a Internet, los derechos a la intimidad y la protección de datos;

20. Insta a la UE a que luche contra la penalización del uso de herramientas de cifrado, evasión de la censura y protección de la intimidad por parte de los defensores de los derechos humanos, negándose a limitar el uso del cifrado dentro de la UE y a que se oponga a los gobiernos de terceros países que imputen a los defensores de los derechos humanos por dichos motivos;

21. Insta a la UE a que luche contra la penalización del uso de herramientas de cifrado, evasión de la censura y protección de la intimidad, negándose a limitar el uso del cifrado dentro de la UE y oponiéndose a los gobiernos de terceros países que penalicen dichas herramientas;

22. Hace hincapié en que la efectividad de la política de la UE en materia de desarrollo y de derechos humanos exigirá la integración generalizada de la consideración de las TIC y la reducción de la brecha digital, proporcionando infraestructuras tecnológicas básicas, facilitando el acceso al conocimiento y a la información para promover las competencias digitales y promoviendo la utilización de normas abiertas en los documentos y el uso de *software* gratuito y de fuente abierta, en su caso, para garantizar la apertura y la transparencia (sobre todo por parte de los organismos públicos) —incluida la garantía de la protección de datos en el ámbito digital en todo el mundo—, así como una mejor comprensión de los riesgos y beneficios potenciales de las TIC;

23. Pide a la Comisión que apoye la supresión de las barreras digitales para las personas con discapacidad; considera de enorme importancia que las políticas de la UE en materia de desarrollo y fomento de los derechos humanos en el mundo persigan mitigar la brecha digital para las personas con discapacidad y ofrecer un marco más amplio de derechos, en especial por lo que respecta al acceso al conocimiento, la participación digital y la inclusión en las nuevas oportunidades económicas y sociales que brinda Internet;

24. Subraya que la recopilación y difusión digital legítima de pruebas de violaciones de los derechos humanos puede contribuir a la lucha contra la impunidad y el terrorismo en todo el mundo; opina que este material debe ser admisible como prueba en casos debidamente justificados en el marco de la legislación (penal) internacional, en los procedimientos judiciales, con arreglo a las garantías internacionales, regionales y constitucionales; recomienda la creación de mecanismos en el ámbito del Derecho penal internacional para establecer procedimientos mediante los cuales obtener y recabar dichos datos para facilitar las pruebas necesarias en los procedimientos judiciales;

25. Lamenta el hecho de que algunos servicios y tecnologías de la información y la comunicación producidos en la UE se vendan y puedan ser utilizados en terceros países por particulares, empresas y administraciones públicas con la intención específica de conculcar los derechos humanos mediante la censura, la vigilancia masiva, la interferencia intencionada, la intercepción y la vigilancia, y por medio del seguimiento y el rastreo de ciudadanos y de sus actividades en las redes de telefonía (móvil) e Internet; manifiesta su preocupación por que algunas empresas con sede en la UE puedan ofrecer tecnologías y servicios que puedan permitir tales violaciones de los derechos humanos;

26. Observa que las amenazas para la seguridad de la Unión Europea y sus Estados miembros y terceros países suelen proceder de individuos o grupos reducidos que utilizan redes de comunicación digital para planear y perpetrar ataques, y que los instrumentos y tácticas necesarios para superar tales amenazas han de ser constantemente objeto de revisión y actualización;

27. Considera que la vigilancia masiva no justificada por el aumento del riesgo de atentados y amenazas terroristas contraviene los principios de necesidad y proporcionalidad y, por tanto, constituye una vulneración de los derechos humanos;

28. Insta a los Estados miembros a que fomenten un pleno control democrático de las operaciones de los servicios de inteligencia en terceros países y verifiquen la plena conformidad de dichas operaciones con el Estado de Derecho, y a que pidan cuentas a los servicios y particulares de las operaciones efectuadas de forma ilícita;

29. Anima a los Estados miembros a que, en vista de la mayor cooperación e intercambio de información entre Estados miembros y terceros países, también mediante la utilización de la vigilancia digital, garanticen el control democrático de esos servicios y de sus actividades a través de una adecuada supervisión interna, ejecutiva, judicial y parlamentaria independiente;

30. Subraya que los principios de la responsabilidad social de las empresas y los criterios de consideración de los derechos humanos en la etapa de diseño, que constituyen soluciones tecnológicas e innovaciones para la protección de tales derechos, deben adoptarse en la legislación de la UE con el fin de garantizar que los proveedores de servicios de Internet, los desarrolladores de *software*, los productores de equipos informáticos, los servicios y medios de las redes sociales, los operadores de telefonía móvil y otros interlocutores tengan en cuenta los derechos humanos de los usuarios finales a escala mundial;

31. Insta a la UE a que garantice una mayor transparencia en la relación entre los operadores de telefonía móvil o los proveedores de servicios de Internet y los gobiernos, y a que exija esta transparencia en sus relaciones con terceros países, requiriendo a los citados operadores y proveedores la publicación de informes anuales detallados sobre transparencia, que incluyan informes sobre las acciones solicitadas por las autoridades, así como sobre los vínculos financieros existentes entre los poderes públicos y los operadores o proveedores interesados;

32. Recuerda a los agentes empresariales la responsabilidad que tienen de respetar los derechos humanos en todas sus operaciones mundiales, con independencia de la ubicación de sus usuarios y de si el Estado de acogida cumple sus propias obligaciones en materia de derechos humanos; pide a las empresas de TIC, en particular a las que tienen sede en la UE, que apliquen los Principios Rectores de las Naciones Unidas sobre las empresas y los derechos humanos, también mediante la adopción de medidas de diligencia debida y medidas de salvaguardia con respecto a la gestión de riesgos, así como mediante la facilitación de soluciones efectivas cuando sus actividades hayan supuesto un menoscabo de los derechos humanos o contribuido al mismo;

33. Incide en la necesidad de velar por la aplicación y el seguimiento de la normativa y las sanciones de la UE en lo que atañe a las TIC de forma más eficaz, incluida la utilización de mecanismos de intervención generalizada, con el fin de garantizar que todas las partes, incluidos los Estados miembros, se atengan a la legislación y se preserve la igualdad de condiciones;

34. Hace hincapié en que el respeto de los derechos fundamentales resulta crucial para el éxito de las políticas antiterroristas, incluida la utilización de tecnologías de vigilancia digital;

35. Acoge con satisfacción la decisión adoptada en la sesión plenaria del Arreglo de Wassenaar de diciembre de 2013 con respecto a los controles de las exportaciones en los ámbitos de los instrumentos policiales, de vigilancia y de recopilación de información y de los sistemas de vigilancia de red; recuerda la aún muy incompleta naturaleza del régimen de la UE sobre productos de doble uso y, en particular, del Reglamento de la UE a este respecto, en lo concerniente al control eficaz y sistemático de las exportaciones de TIC nocivas a países no democráticos;

36. Insta a la Comisión, en el contexto de la próxima revisión y renovación de la política sobre productos de doble uso, a que formule a la mayor brevedad una propuesta de políticas inteligentes y eficaces para limitar y regular la exportación comercial de servicios en relación con la instalación y utilización de las denominadas tecnologías de doble uso, abordando las exportaciones potencialmente dañinas de productos y servicios de TIC a terceros países, conforme se convino en la Declaración Común del Parlamento Europeo, el Consejo y la Comisión de abril de 2014; pide a la Comisión que disponga las garantías pertinentes para evitar que estos controles de las exportaciones redunden en perjuicio de la investigación, incluidas la investigación científica y la investigación de seguridad informática;

37. Hace hincapié en que la Comisión debe, en breve plazo, ser capaz de proporcionar a las empresas que duden si solicitar una licencia de exportación información actualizada en tiempo real sobre la legalidad o los efectos potencialmente perjudiciales de las posibles transacciones;

38. Pide a la Comisión que presente propuestas para revisar el modo en que podrían utilizarse las normas de la UE relativas a las TIC con el fin de prevenir los efectos potencialmente dañinos de la exportación de tales tecnologías u otros servicios a terceros países donde conceptos como la «intercepción lícita» no pueden considerarse equivalentes a los de la Unión Europea, o, por ejemplo, que tienen un historial deficiente en materia de derechos humanos o en los que no existe el Estado de Derecho;

39. Reitera que las normas de la UE, en particular la Carta de los Derechos Fundamentales de la Unión Europea, deben prevalecer a la hora de evaluar los incidentes que impliquen tecnologías de doble uso utilizadas de formas que puedan restringir los derechos humanos;

40. Aboga por el desarrollo de políticas que regulen las ventas de «ataques de día cero» y vulnerabilidades, al objeto de evitar su utilización en ciberataques o para el acceso no autorizado a dispositivos que dé lugar a violaciones de los derechos humanos, sin que dichas medidas regulatorias repercutan de forma significativa en la investigación académica o en cualquier otro tipo de investigación legítima en materia de seguridad;

41. Lamenta la cooperación activa de ciertas empresas europeas, y de determinadas empresas internacionales que comercian con tecnologías de doble uso con posibles repercusiones negativas para los derechos humanos y operan en la UE, con regímenes cuyas acciones vulneran los derechos humanos;

42. Insta a la Comisión a que excluya públicamente a las empresas que realicen tales actividades de los procesos de contratación de la UE, de la financiación a la investigación y el desarrollo y de cualquier otra forma de ayuda económica;

43. Pide a la Comisión que preste especial atención a los aspectos de los derechos humanos en los procesos de contratación pública de equipos tecnológicos, sobre todo en países cuyas prácticas en dicho ámbito carezcan de fiabilidad;

44. Pide a la Comisión y al Consejo que defiendan activamente un Internet abierto, los procedimientos de toma de decisiones en los que intervienen múltiples interlocutores, la neutralidad de la red, las libertades digitales y las garantías de protección de datos en terceros países a través de los foros de gobernanza de Internet;

45. Condena el debilitamiento y menoscabo de los protocolos y productos de cifrado, sobre todo por parte de los servicios de inteligencia que tratan de interceptar comunicaciones cifradas;

46. Desaconseja la privatización de las funciones coercitivas a través de empresas de Internet y proveedores de servicios de Internet;

47. Pide que se aclaren las normas y estándares que utilizan los agentes privados para desarrollar sus sistemas;

48. Reitera la importancia de evaluar el contexto en que se utilizan las tecnologías, a fin de determinar por completo su repercusión en los derechos humanos;

49. Pide explícitamente que se promuevan herramientas que permitan utilizar Internet de forma anónima o seudónima y se opone al punto de vista parcial de que dichas herramientas permiten el desarrollo de actividades delictivas, en lugar de capacitar a los activistas de los derechos humanos dentro y fuera de la UE;

50. Insta al Consejo, a la Comisión y al SEAE a que elaboren políticas inteligentes y eficaces para regular la exportación de tecnologías de doble uso, abordando las exportaciones potencialmente nocivas de productos y servicios de TIC, a escala internacional y en el marco de regímenes multilaterales de control de las exportaciones y otros organismos internacionales;

51. Subraya que ninguna modificación de la normativa con objeto de aumentar la eficacia de los controles de las exportaciones con respecto a las transferencias intangibles de tecnología debe impedir la investigación legítima ni el acceso a información y el intercambio de la misma, y que ninguna de las posibles medidas, como el uso de autorizaciones generales de exportación de la UE para investigación de doble uso, debería tener un efecto disuasorio en las personas físicas o las pymes;

52. Pide a los Estados miembros que garanticen que las políticas actuales y futuras sobre el control de las exportaciones no restrinjan las actividades de investigadores legítimos de seguridad, y que los controles de las exportaciones se apliquen de buena fe y solo a tecnologías claramente definidas que vayan a utilizarse para la vigilancia masiva, la censura, la interferencia intencionada, la intercepción y la supervisión, y el seguimiento y rastreo de ciudadanos y de sus actividades en las redes de telefonía (móvil);

53. Recuerda que las tecnologías inalámbricas *ad hoc* en malla ofrecen grandes posibilidades para facilitar redes auxiliares en zonas donde no haya Internet o este haya sido bloqueado, y pueden contribuir al fomento de los derechos humanos;

54. Pide a la Comisión que designe a un grupo independiente de expertos que pueda llevar a cabo una evaluación de impacto en materia de derechos humanos de las normas vigentes de la UE para las TIC, con el fin de formular recomendaciones de ajustes que aumentarán la protección de los derechos humanos, sobre todo cuando los sistemas se exporten;

55. Reconoce que el avance tecnológico plantea un reto a los ordenamientos jurídicos y requiere su adaptación a las nuevas circunstancias; destaca la importancia de que los legisladores presten más atención a las cuestiones relacionadas con la economía digital;

56. Pide a la Comisión que procure la implicación en estas tareas de la sociedad civil, así como de expertos independientes, incluidos investigadores de seguridad, en el ámbito de las TIC en terceros países, con el fin de garantizar la disposición de unos conocimientos técnicos actualizados que den lugar a la formulación de políticas que sigan siendo válidas en el futuro;

57. Subraya la necesidad de evitar consecuencias no deseadas, como las restricciones o los efectos disuasorios respecto a la investigación y el desarrollo científicos y demás tipos de investigación y desarrollo de buena fe, al intercambio de información y al acceso a la misma, al desarrollo de conocimientos en materia de seguridad o a la exportación de tecnologías que contribuyan a la adquisición de las competencias digitales necesarias y al fomento de los derechos humanos;

58. Cree que la cooperación entre las administraciones y los agentes privados en todo el mundo en el ámbito digital, incluyendo el Foro de Gobernanza de Internet, exige controles y equilibrios inequívocos, y no debe dar lugar al menoscabo de la supervisión democrática y judicial;

59. Destaca que la voluntariedad no basta, sino que se requieren disposiciones vinculantes para hacer que las empresas tomen en consideración el historial en materia de derechos humanos de los países antes de vender en ellos sus productos y que lleven a cabo una evaluación del efecto que tendrán sus tecnologías sobre los defensores de los derechos humanos y las personas críticas con el Gobierno;

60. Opina que la exportación de productos altamente sensibles debe evaluarse antes de que dichos productos abandonen la UE, y que se requieren sanciones en caso de infracción.

61. Pide que se reconozca el derecho al cifrado de cada individuo y que se creen las condiciones necesarias para permitir el cifrado; considera que el usuario final debe tener el control, para lo cual necesitará las capacidades necesarias para poder ejercer adecuadamente dicho control;

62. Pide la introducción de normas de cifrado de extremo a extremo (*end-to-end*) como requisito fundamental para todos los servicios de comunicación con el fin de que los gobiernos, los servicios secretos y los órganos de vigilancia tengan más dificultad para conocer los contenidos de las comunicaciones;

63. Subraya la responsabilidad especial de los servicios secretos estatales de generar confianza, y pide que se ponga fin a la vigilancia masiva; considera que debe abordarse y detenerse la supervisión de ciudadanos europeos a través de servicios secretos nacionales y extranjeros.

64. Rechaza la venta y distribución de tecnologías de vigilancia europeas e instrumentos de censura a regímenes autoritarios en los que no existe el Estado de Derecho;

65. Pide que se amplíen las oportunidades de protección internacional de denunciantes y anima a los Estados miembros a que elaboren leyes para protegerlos;

66. Pide un representante de las Naciones Unidas para las libertades digitales y la protección de datos y que se amplíe el ámbito de competencia del comisario de la UE para los derechos humanos de manera que también se tenga en cuenta la tecnología desde el punto de vista de los derechos humanos;

67. Pide medidas que garanticen la protección de la intimidad de activistas, periodistas y ciudadanos en cualquier lugar del mundo y que estos puedan interrelacionarse a través de Internet;

68. Insiste en que debe reconocerse el acceso a Internet como uno de los derechos humanos y pide medidas para eliminar la brecha digital;

69. Encarga a su Presidente que transmita la presente Resolución al Consejo, a la Comisión y a la Vicepresidenta de la Comisión/Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad y al SEAE.