Europäisches Parlament
2014 - 2019

ANGENOMMENE TEXTE

P8_TA(2015)0288

Menschenrechte und Technologie in Drittstaaten

Entschließung des Europäischen Parlaments vom 8. September 2015 zu dem Thema „Menschenrechte und Technologie: die Auswirkungen von Systemen zur Ausspähung und Überwachung auf die Menschenrechte in Drittstaaten“ (2014/2232(INI))

Das Europäische Parlament,

– unter Hinweis auf die Allgemeine Erklärung der Menschenrechte und den Internationalen Pakt über bürgerliche und politische Rechte, insbesondere dessen Artikel 19,

– unter Hinweis auf den Strategischen Rahmen der Europäischen Union für Menschenrechte und Demokratie, den der Rat am 25. Juni 2012 angenommen hat[1],

– unter Hinweis auf die Menschenrechtsleitlinien der EU in Bezug auf die Freiheit der Meinungsäußerung – online und offline, die vom Rat „Auswärtige Angelegenheiten“ am 12. Mai 2014 angenommen wurden[2],

– unter Hinweis auf den von der Kommission im Juni 2013 veröffentlichten Leitfaden für den IKT-Sektor zur Umsetzung der Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte („ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights“),

– unter Hinweis auf den Bericht der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) vom 15. Dezember 2011 über Meinungsfreiheit im Internet („Freedom of Expression on the Internet“)[3] und auf den regelmäßigen Bericht der Beauftragten der OSZE für Medienfreiheit vom 27. November 2014 an den Ständigen Rat der OSZE[4],

– unter Hinweis auf den Bericht des Sonderberichterstatters der Vereinten Nationen über den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des

---

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 .

Terrorismus vom 23. September 2014 (A/69/397)[1],

– unter Hinweis auf den Bericht des Amts des Hohen Kommissars der Vereinten Nationen für Menschenrechte vom 30. Juni 2014 zum Recht auf Privatsphäre im digitalen Zeitalter („The right to privacy in the digital age“)[2],

– unter Hinweis auf den Bericht des Sonderberichterstatters der Vereinten Nationen über die Förderung und den Schutz der Meinungsfreiheit und des Rechts der freien Meinungsäußerung vom 17. April 2013 (A/HRC/23/40), in dem die Auswirkungen der staatlichen Überwachung der Kommunikation auf die Ausübung der Menschenrechte auf Privatsphäre, auf Meinungsfreiheit und freie Meinungsäußerung analysiert werden,

– unter Hinweis auf den Bericht des Ausschusses für Recht und Menschenrechte der Parlamentarischen Versammlung des Europarates vom 26. Januar 2015 über das Thema Massenüberwachung[3],

– unter Hinweis auf seine Entschließung vom 12. März 2014 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, die Überwachungsbehörden in mehreren Mitgliedstaaten und die entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres[4],

– unter Hinweis auf den Bericht des Sondergesandten des Generalsekretärs der Vereinten Nationen für die Frage der Menschenrechte und transnationaler Unternehmen sowie anderer Wirtschaftsunternehmen vom 21. März 2011 mit dem Titel „Leitprinzipien für Wirtschaft und Menschenrechte: Umsetzung des Rahmens der Vereinten Nationen ‚Schutz, Achtung und Abhilfe‘“ („Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework“)[5],

– unter Hinweis auf die Leitlinien der OSZE für multinationale Unternehmen[6] und den Jahresbericht 2014 über die Leinlinien der OSZE für multinationale Unternehmen[7],

– unter Hinweis auf den Jahresbericht 2013 der Zentralstelle für die Vergabe von Internet-Namen und -Adressen[8],

– unter Hinweis auf die Mitteilung der Kommission an das Europäische Parlament, den

---

1 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement.
2 http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc.
3 http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2.
4 Angenommene Texte, P7_TA(2014)0230.
5 http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf?v=1392752313000/_/jcr:system/jcr:versionstorage/12/52/13/125213a0-e4bc-4a15-bb96-9930bb8fb6a1/1.3/jcr:frozennode.
6 http://www.oecd.org/daf/inv/mne/48004323.pdf.
7 http://www.oecd-ilibrary.org/docserver/download/2014091e.pdf?expires=1423160236&id=id&accname=ocid194994&checksum=D1FC664FBCEA28FC856AE63932715B3C.
8 https://www.icann.org/en/system/files/files/annual-report-2013-en.pdf.

Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 12. Februar 2014 mit dem Titel „Internet-Politik und Internet-Governance: Europas Rolle bei der Mitgestaltung der Zukunft der Internet-Governance“[1],

– unter Hinweis auf die am 24. April 2014 von der Konferenz NETmundial angenommene Erklärung (NETmundial Multistakeholder Statement)[2],

– unter Hinweis auf die Zusammenfassung des Vorsitzenden betreffend die neunte Tagung des Internet Governance Forum, die von 2.–5. September 2014 in Istanbul stattfand,

– unter Hinweis auf die restriktiven Maßnahmen der Europäischen Union, wobei diese Maßnahmen in einigen Fällen Embargos auf Telekommunikationsgeräte, Informations- und Kommunikationstechnologien (IKT) und Überwachungsinstrumente umfassen,

– unter Hinweis auf die Verordnung (EU) Nr. 599/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 zur Änderung der Verordnung (EG) Nr. 428/2009 des Rates über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck[3],

– unter Hinweis auf die Gemeinsame Erklärung des Europäischen Parlaments, des Rates und der Kommission vom 16. April 2014 über die Überarbeitung des Systems zur Kontrolle der Ausfuhr von Gütern mit doppeltem Verwendungszweck[4],

– unter Hinweis auf die Beschlüsse der 19. Plenartagung des Wassenaar-Abkommens über Ausfuhrkontrollen für konventionelle Waffen sowie Güter und Technologien mit doppeltem Verwendungszweck, die von 3.bis 4. Dezember 2013 in Wien stattfand,

– unter Hinweis auf die Mitteilung der Kommission an den Rat und das Europäische Parlament vom 24. April 2014 mit dem Titel „Die Überprüfung der Ausfuhrkontrollpolitik: in einer Welt des Wandels Sicherheit und Wettbewerbsfähigkeit gewährleisten“[5],

– unter Hinweis auf die Schlussfolgerungen des Rates vom 21. November 2014 zur Überprüfung der Ausfuhrkontrollpolitik,

– unter Hinweis auf seine Entschließung vom 11. Dezember 2012 zu einer digitalen Freiheitsstrategie in der Außenpolitik der EU[6],

– unter Hinweis auf seine Entschließung vom 13. Juni 2013 zur Presse- und Medienfreiheit in der Welt[7],

– unter Hinweis auf alle von ihm angenommenen Entschließungen zu dringlichen Fällen

---

1 COM(2014)0072.
2 http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.
3 ABl. L 173 vom 12.6.2014, S. 79.
4 ABl. L 173 vom 12.6.2014, S. 82.
5 COM(2014)0244.
6 Angenommene Texte, P7_TA(2012)0470.
7 Angenommene Texte, P7_TA(2013)0274.

der Verletzung der Menschenrechte, der Demokratie und der Rechtsstaatlichkeit, in denen Bedenken in Bezug auf digitale Freiheiten geäußert werden,

– unter Hinweis auf seine Entschließung vom 12. März 2015 zu den Prioritäten der EU für den Menschenrechtsrat der Vereinten Nationen im Jahr 2015[1],

– unter Hinweis auf seine Entschließung vom 11. Februar 2015 zu der Verlängerung des Mandats des Internet Governance Forum[2],

– unter Hinweis auf seine Entschließung vom 12. März 2015 zu dem Jahresbericht 2013 über Menschenrechte und Demokratie in der Welt und die Politik der Europäischen Union in diesem Bereich[3],

– unter Hinweis auf die an den LIBE-Ausschuss gerichtete schriftliche Aussage Edward Snowdens vom März 2014[4],

– unter Hinweis auf die Europäische Menschenrechtskonvention und die laufenden Verhandlungen zum Beitritt der EU zu dieser Konvention,

– unter Hinweis auf die Charta der Grundrechte der Europäischen Union,

– gestützt auf Artikel 52 seiner Geschäftsordnung,

– unter Hinweis auf den Bericht des Ausschusses für auswärtige Angelegenheiten (A8-0178/2015),

A. in der Erwägung, dass technologische Entwicklungen und der Zugang zum offenen Internet im Hinblick auf die Förderung der Durchsetzung der Menschenrechte und Grundfreiheiten und die Gewährleistung der umfassenden Achtung dieser Rechte und Freiheiten zunehmend von Bedeutung sind, was positive Folgen zeitigt, da somit das Recht auf freie Meinungsäußerung, der Zugang zu Informationen, das Recht auf Privatsphäre und die Versammlungs- und Vereinigungsfreiheit weltweit in Anspruch genommen werden können;

B. in der Erwägung, dass Technologien allerdings als Instrumente missbraucht werden können, mit denen im Zuge von Zensur und Überwachung, des unbefugten Zugangs zu Geräten, von Störmaßnahmen und Abhörmaßnahmen sowie der Verfolgung und Ortung von Informationen und Personen gegen die Menschenrechte verstoßen wird;

C. in der Erwägung, dass diese Vorgehensweisen von öffentlichen und privaten Akteuren, einschließlich Regierungen und Strafverfolgungsbehörden, sowie auch von kriminellen Vereinigungen und Terrornetzwerken verfolgt und in diesem Rahmen Menschenrechtsverstöße begangen werden;

---

1 Angenommene Texte, P8_TA(2015)0079.
2 Angenommene Texte, P8_TA(2015)0033.
3 Angenommene Texte, P8_TA(2015)0076.
4 http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

D. in der Erwägung, dass der Zusammenhang, in dem IKT konzipiert und genutzt werden, in hohem Maße dafür ausschlaggebend ist, inwiefern sie als Mittel zur Förderung der Menschenrechte oder dazu genutzt werden können, ebendiese Rechte zu verletzen; in der Erwägung, dass es sich bei Informationstechnologien und insbesondere bei Software nur selten um Güter mit nur einem Verwendungszweck und für gewöhnlich um Güter mit doppeltem Verwendungszweck handelt, was deren Potenzial im Hinblick auf die Verletzung von Menschenrechten angeht, während Software allerdings auch eine Form der Sprache darstellt;

E. in der Erwägung, dass IKT bei der Organisation sozialer Bewegungen und von Protesten in verschiedenen Ländern, insbesondere in Ländern unter autoritärem Regime, eine Schlüsselrolle gespielt haben;

F. in der Erwägung, dass die Bewertung der Auswirkungen, die sich aus dem Zusammenhang, in dem Technologien genutzt werden, auf die Menschenrechte ergeben, darauf beruht, inwiefern die Nutzung von Technologien in den nationalen und regionalen Rechtsrahmen reguliert ist, sowie darauf, inwiefern es den politischen Institutionen und dem Justizwesen möglich ist, diese Nutzung zu überwachen;

G. in der Erwägung, dass Privatakteure in der digitalen Sphäre in allen Bereichen gesellschaftlicher Aktivitäten zwar eine immer wichtigere Rolle spielen, es allerdings nach wie vor keine Schutzvorkehrungen gibt, damit sie die Grundrechte und Grundfreiheiten nicht übermäßig einschränken; in der Erwägung, dass Privatakteure in der Folge eine aktivere Rolle einnehmen, was die Bewertung der Rechtmäßigkeit von Inhalten und die Entwicklung von Cyber-Sicherheitssystemen und Überwachungssystemen angeht, was sich auf die Menschenrechte in aller Welt schädlich auswirken kann;

H. in der Erwägung, dass das Internet revolutionär ist, was die Möglichkeiten des Austauschs von Daten, Informationen und Wissen aller Art angeht;

I. in der Erwägung, dass die Verschlüsselung eine wichtige Methode ist, mit der sowohl Kommunikationsprozesse als auch die daran beteiligten Personen geschützt werden können;

J. in der Erwägung, dass sich die Tatsache, dass die Entscheidungsfindung im Rahmen eines Modells der Beteiligung verschiedener Interessenträger erfolgt, positiv auf die Verwaltung des Internets ausgewirkt hat, wobei es sich um ein Verfahren handelt, bei dem für eine sinnvolle, inklusive Beteiligung aller Interessenträger, einschließlich Regierungen, Zivilgesellschaften, technischer und akademischer Kreise, des Privatsektors und der Nutzer, sowie für eine entsprechende Rechenschaftspflicht gesorgt ist;

K. in der Erwägung, dass Nachrichtendienste Verschlüsselungsprotokolle und -produkte systematisch unterlaufen, um den Daten- und Kommunikationsverkehr ausspähen zu können; in der Erwägung, dass die Nationale Sicherheitsagentur der Vereinigten Staaten (National Security Agency – NSA) zu einer Vielzahl sogenannter „Zero-Day-Exploits“ – Sicherheitslücken in der IT-Sicherheit, die der Öffentlichkeit oder dem Produktanbieter noch unbekannt sind – Informationen gesammelt hat; in der Erwägung, dass derartige Aktivitäten die globalen Bemühungen zur Verbesserung der IT-Sicherheit untergraben;

L. in der Erwägung, dass in der EU ansässige Nachrichtendienste Tätigkeiten nachgehen, die gegen die Menschenrechte verstoßen;

M. in der Erwägung, dass die justizielle und demokratische Kontrolle und entsprechende Schutzvorkehrungen angesichts der raschen technologischen Entwicklungen stark unterentwickelt sind;

N. in der Erwägung, dass (Cyber-)Sicherheit und Maßnahmen zur Bekämpfung des Terrorismus, in deren Rahmen IKT eingesetzt werden, und die Überwachung des Internets sich schädlich auf die Menschenrechte und die Individualrechte von Personen in aller Welt auswirken können – wovon auch Unionsbürger betroffen sein können, etwa wenn sie im Ausland ansässig sind oder reisen–, insbesondere wenn es diesbezüglich keine rechtliche Grundlage gibt, die auf den Grundsätzen der Notwendigkeit und der Verhältnismäßigkeit sowie auf demokratischer und justizieller Überwachung beruht;

O. in der Erwägung, dass Internetfilter und die Kommunikationsüberwachung Menschenrechtsverteidiger daran hindern, sich des Internets zu bedienen und vertrauliche Informationen zu übermitteln, und dass damit gegen mehrere Artikel der Allgemeinen Erklärung der Menschenrechte verstoßen wird, in deren Rahmen allen Menschen das Recht auf Privatsphäre sowie jenes auf freie Meinungsäußerung gewährt wird;

P. in der Erwägung, dass sowohl digitale Sicherheit als auch digitale Freiheit wesentlich sind und einander nicht ersetzen können, sondern einander vielmehr stärken sollten;

Q. in der Erwägung, dass die Europäische Union im Bereich der digitalen Freiheiten nur beispielgebend sein kann, wenn diese Freiheiten auch in der EU selbst geschützt werden, weswegen es entscheidend ist, dass das EU-Datenschutzpaket angenommen wird;

R. in der Erwägung, dass weitreichende gesellschaftliche Interessen auf dem Spiel stehen, beispielsweise der Schutz grundlegender Rechte, und dass diese Interessen nicht allein dem Markt überlassen werden dürfen, sondern reguliert werden müssen;

S. in der Erwägung, dass die Wahrung der Grundrechte und der Rechtsstaatlichkeit sowie eine wirksame parlamentarische Kontrolle der Nachrichtendienste, die digitale Überwachungstechnologien nutzen, wichtige Elemente der internationalen Zusammenarbeit darstellen;

T. in der Erwägung, dass auf in der EU ansässige Unternehmen ein großer Anteil des Weltmarkts für IKT entfällt, insbesondere was die Ausfuhr von Technologien zur Überwachung, Ortung, Ausspähung und Kontrolle angeht;

U. in der Erwägung, dass die Einführung von Ausfuhrkontrollen weder zu einer Beeinträchtigung der rechtmäßigen Erforschung von IT-Sicherheitsfragen noch der Entwicklung von IT-Sicherheitsinstrumenten, die nicht mit kriminellen Absichten einhergehen, führen darf;

1. erkennt an, dass die Menschenrechte und die Grundfreiheiten universell sind und in allen ihren Ausdrucksformen weltweit verteidigt werden müssen; betont, dass die Überwachung von Kommunikationsprozessen per se dem Recht auf Privatsphäre und dem Recht auf Meinungsfreiheit zuwiderläuft, wenn dabei keinem angemessenen

Rechtsrahmen Rechnung getragen wird;

2. fordert die Kommission auf, dafür zu sorgen, dass das auswärtige Handeln der EU und ihre internen politischen Maßnahmen in Bezug auf IKT übereinstimmen;

3. vertritt die Auffassung, dass die aktive Komplizenschaft bestimmter Mitgliedstaaten der EU an der Massenüberwachung der Bürger und der Ausspionierung politischer Führungspersönlichkeiten durch die NSA, wie sie von Edward Snowden enthüllt wurden, der Glaubwürdigkeit der Menschenrechtspolitik der EU schwer geschadet und das weltweit herrschende Vertrauen in die Vorteile der IKT unterlaufen haben;

4. erinnert die Mitgliedstaaten und die betroffenen Agenturen der EU, einschließlich Europol und Eurojust, an ihre sich aus der Charta der Grundrechte der Europäischen Union und im Einklang mit den internationalen Menschenrechtsnormen und den Zielen des auswärtigen Handelns der EU ergebenden Verpflichtungen, keine nachrichtendienstlichen Daten weiterzugeben, die zu Menschenrechtsverletzungen in einem Drittland führen könnten, und auch keine Informationen zu nutzen, die infolge von Menschenrechtsverletzungen außerhalb der EU gewonnen wurden, beispielsweise also durch rechtswidrige Überwachung;

5. betont, dass die Auswirkungen von Technologien in Bezug auf eine verbesserte Menschenrechtslage bei allen einschlägigen Maßnahmen und Programmen der EU berücksichtigt werden sollten, um den Schutz der Menschenrechte zu fördern und auch die Förderung von Demokratie, Rechtsstaatlichkeit und verantwortungsvoller Regierungsführung sowie friedlicher Konfliktlösung voranzubringen;

6. fordert, dass aktiv Technologien entwickelt und verbreitet werden, mit deren Hilfe zum Schutz der Menschenrechte und zur Durchsetzung der digitalen Rechte, Freiheiten und Sicherheiten der Menschen beigetragen werden kann und mit denen bewährte Verfahren und angemessene Rechtsrahmen gefördert werden und die Sicherheit und Integrität personenbezogener Daten gewährleistet wird; fordert insbesondere die EU und ihre Mitgliedstaaten nachdrücklich auf, die globale Nutzung und Entwicklung offener Standards sowie freier, quelloffener Software und entsprechender Verschlüsselungstechnologien zu fördern;

7. fordert die EU auf, Akteure vermehrt zu fördern, die an der Stärkung der Datenschutz- und Datensicherheitsstandards von IKT auf allen Ebenen, unter anderem in Bezug auf Hardware, Software und Kommunikationsstandards sowie die Entwicklung von Hardware und Software im Rahmen eines eingebauten Datenschutzes, arbeiten;

8. fordert, dass im Rahmen der Europäischen Initiative für Demokratie und Menschenrechte ein Fonds für Menschenrechte und Technologie eingerichtet wird;

9. fordert die EU und insbesondere den EAD nachdrücklich auf, ihre Kommunikation mit Menschenrechtsverteidigern zu verschlüsseln, um diese nicht in Gefahr zu bringen und ihre eigene Kommunikation mit Externen vor Überwachung zu schützen;

10. fordert die EU auf, freie, quelloffene Software zu implementieren und anderen Akteuren nahezulegen, es ihr gleichzutun, da mit derartiger Software für mehr Sicherheit und eine stärkere Achtung der Menschenrechte gesorgt wäre;

11. weist darauf hin, dass IKT in Konfliktgebieten entwickelt werden müssen, um friedensschaffende Maßnahmen zu fördern und zu erreichen, dass die an der friedlichen

Konfliktlösung beteiligten Parteien sicher kommunizieren können;

12. fordert, dass Bedingungen, Bezugswerte und Meldeverfahren umgesetzt werden, damit es durch die finanzielle und technische Unterstützung, die die EU hinsichtlich der Entwicklung neuer Technologien in Drittländern leistet, nicht zu Menschenrechtsverletzungen kommt;

13. fordert die Kommission und den Rat auf, aktiv mit Regierungen von Drittländern zusammenzuarbeiten und Menschenrechtsverteidiger, Aktivisten der Zivilgesellschaft und unabhängige Journalisten mithilfe vorhandener europäischer Unterstützungsmechanismen und politscher Instrumente auch weiterhin zu unterstützen, zu schulen und zu stärken, was die sichere Nutzung von IKT im Rahmen ihrer Aktivitäten angeht, und die diesbezüglichen Grundrechte in Bezug auf die Privatsphäre, wie etwa den ungehinderten Zugang zu den Informationsflüssen im Internet, das Recht auf Privatsphäre und Datenschutz sowie freie Meinungsäußerung, Versammlungsfreiheit, Vereinigungsfreiheit, Pressefreiheit und Veröffentlichungsfreiheit im Internet zu fördern;

14. weist auf die Not von Whistleblowern und ihren Unterstützern, einschließlich Journalisten, infolge ihrer Enthüllungen von rechtswidrigen Überwachungspraktiken in Drittländern hin; vertritt die Auffassung, dass solche Einzelpersonen als Menschenrechtsverteidiger gelten und daher den Schutz der EU genießen sollten, wie es gemäß den Leitlinien der EU betreffend den Schutz von Menschenrechtsverteidigern vorgesehen ist; weist die Kommission und die Mitgliedstaaten erneut darauf hin, dass sie die Möglichkeit eingehend prüfen sollten, Whistleblowern internationalen Schutz vor strafrechtlicher Verfolgung zu gewähren;

15. bedauert, dass Sicherheitsmaßnahmen, einschließlich Maßnahmen zur Bekämpfung des Terrorismus, zunehmend als Vorwand für die Verletzung des Rechts auf Privatsphäre und für ein hartes Durchgreifen angesichts rechtmäßiger Tätigkeiten von Menschenrechtsverteidigern, Journalisten und politischen Aktivisten dienen; weist erneut darauf hin, dass es der tiefen Überzeugung ist, dass die nationale Sicherheit niemals als Rechtfertigung für eine ungezielte, im Geheimen erfolgende oder massenhafte Überwachung gelten darf; besteht darauf, dass bei derartigen Maßnahmen der Rechtsstaatlichkeit und den Menschenrechtsnormen, einschließlich des Rechts auf Privatsphäre und auf Datenschutz, voll und ganz Rechnung getragen wird;

16. fordert den EAD und die Kommission auf, in ihren politischen Dialogen mit Drittländern und ihren Programmen für die Entwicklungszusammenarbeit darauf hinzuwirken, die demokratische Kontrolle der Sicherheits- und Nachrichtendienste zu stärken; fordert die Kommission nachdrücklich auf, Organisationen der Zivilgesellschaft und Legislativorgane in Drittländern zu unterstützen, die darauf hinarbeiten, die Kontrolle, Transparenz und Rechenschaftspflicht der nationalen Sicherheitsdienste auszuweiten; fordert, dass in dem künftigen Aktionsplan der EU für Menschenrechte und Demokratisierung entsprechende spezifische Zusagen niedergelegt werden;

17. fordert den Rat und die Kommission nachdrücklich auf, die digitalen Freiheiten und den unbeschränkten Zugang zum Internet bei jeglichem Kontakt mit Drittländern, einschließlich Beitrittsverhandlungen, Handelsverhandlungen, Menschenrechtsdialogen und diplomatischen Kontakten, zu fördern;

18. erkennt an, dass das Internet sowohl ein öffentlicher Raum als auch ein Marktplatz geworden ist, für den der freie Informationsfluss und der Zugang zu IKT unverzichtbar geworden sind; betont daher, dass die digitale Freiheit und der digitale Handel sowohl gefördert als auch geschützt werden müssen;

19. fordert, dass in alle Vereinbarungen mit Drittländern Klauseln aufgenommen werden, in denen ausdrücklich darauf verwiesen wird, dass die digitalen Freiheiten, die Netzneutralität, ein unzensierter, unbeschränkter Zugang zum Internet, das Recht auf Privatsphäre und der Datenschutz zu fördern, zu gewährleisten und zu achten sind;

20. fordert die EU nachdrücklich auf, der Kriminalisierung dessen, dass Menschenrechtsverteidiger Instrumente zur Verschlüsselung und zur Umgehung der Zensur sowie zum Schutz der Privatsphäre nutzen, entgegenzutreten, indem sie sich nicht darauf einlässt, die Nutzung von Verschlüsselungsinstrumenten in der EU einzuschränken, und fordert sie auf, das Vorgehen von Drittländern, die gegen Menschenrechtsverteidiger entsprechende Anklagen erheben, in Frage zu stellen;

21. fordert die EU nachdrücklich auf, der Kriminalisierung der Nutzung von Instrumenten zur Verschlüsselung und zur Umgehung der Zensur sowie zum Schutz der Privatsphäre entgegenzutreten, indem sie sich nicht darauf einlässt, die Nutzung von Verschlüsselungsinstrumenten in der EU einzuschränken, und fordert sie auf, das Vorgehen von Drittländern, die die Nutzung entsprechender Instrumente unter Strafe stellen, in Frage zu stellen;

22. betont, dass der Bereich IKT durchgängig berücksichtigt und die digitale Kluft geschlossen werden muss, wenn die Entwicklungs- und Menschenrechtspolitik der EU wirksam sein soll, was durch die Bereitstellung einer grundlegenden technologischen Infrastruktur, die Vereinfachung des Zugangs zu Wissen und Informationen mit dem Ziel, digitale Kompetenzen zu fördern, und durch die Förderung der Nutzung offener Standards in Dokumenten sowie von freier, quelloffener Software erreicht wird, wo dies angezeigt ist, um somit für Offenheit und Transparenz (insbesondere von öffentlichen Institutionen) zu sorgen – einschließlich der Wahrung des Datenschutzes in der digitalen Sphäre weltweit – sowie für ein besseres Verständnis für die möglichen Risiken und den möglichen Nutzen von IKT;

23. fordert die Kommission auf, die Entfernung digitaler Barrieren für Menschen mit Behinderungen zu unterstützen; erachtet es für äußerst wichtig, dass die Politik der EU in Bezug auf die Entwicklung und die Förderung der Menschenrechte darauf abzielt, die digitale Kluft für Menschen mit Behinderungen zu verringern und einen breiteren Rechtsrahmen zu schaffen, insbesondere was den Zugang zu Wissen, die digitale Teilhabe und die Einbeziehung in die neuen wirtschaftlichen und sozialen Möglichkeiten, die das Internet bietet, anbelangt;

24. betont, dass zur weltweiten Bekämpfung der Straflosigkeit und des Terrorismus beigetragen werden kann, indem rechtmäßig Beweise für Menschenrechtsverletzungen digital gesammelt und verbreitet werden; ist der Auffassung, dass das entsprechende Material in Gerichtsverfahren nach internationalem (Straf-)Recht gemäß internationalen, regionalen und verfassungsmäßigen Schutzklauseln in ordnungsgemäß begründeten Fällen als Beweismittel zulässig sein sollte; regt an, im Bereich des internationalen Strafrechts Mechanismen zu schaffen, mit denen Verfahren zur Überprüfung der Echtheit dieser Informationen und zu deren Zusammenstellung eingeführt werden, damit sie als Beweismittel in Gerichtsverfahren eingebracht werden

können;

25. bedauert, dass einige in der EU konzipierte IK-Technologien bzw. von dort erbrachte -Dienstleistungen in Drittländern von Privatpersonen, Unternehmen und Behörden gekauft und genutzt werden können und mit der konkreten Absicht zum Einsatz kommen, die Menschenrechte durch Zensur, Massenüberwachung, Stör-, Abhör- und Kontrollmaßnahmen sowie durch die Verfolgung und Ortung von Bürgern und von deren Aktivitäten in (Mobil-)Telefonnetzen sowie im Internet zu verletzen; ist besorgt darüber, dass einige in der EU ansässige Unternehmen vermutlich Technologien und Dienstleistungen bereitstellen, bei deren Nutzung derartige Menschenrechtsverletzungen begangen werden;

26. stellt fest, dass Bedrohungen der Sicherheit der Europäischen Union und ihrer Mitgliedstaaten sowie von Drittländern oft auf Einzelpersonen oder kleine Gruppen zurückgehen, die digitale Kommunikationsnetzwerke nutzen, um Angriffe zu planen und durchzuführen, und dass die Instrumente und Taktiken, die notwendig sind, um derartige Bedrohungen abzuwenden, ständig überprüft und aktualisiert werden müssen;

27. vertritt die Auffassung, dass Massenüberwachung, die nicht durch ein erhöhtes Risiko eines Terroranschlags oder einer terroristischen Bedrohung gerechtfertigt ist, gegen die Grundsätze Notwendigkeit und Verhältnismäßigkeit und somit auch gegen die Menschenrechte verstößt;

28. fordert die Mitgliedstaaten auf, darauf hinzuwirken, dass die Tätigkeiten von Nachrichtendiensten in Drittländern einer umfassenden demokratischen Kontrolle unterliegen, und sicherzustellen, dass diese Dienste bei ihren Tätigkeiten der Rechtstaatlichkeit vollumfassend Rechnung tragen, und fordert, dass die Dienste und Personen, die bei diesen Tätigkeiten rechtswidrig vorgehen, zur Rechenschaft gezogen werden;

29. fordert die Mitgliedstaaten vor dem Hintergrund der verstärkten Zusammenarbeit und des verstärkten Informationsaustauschs zwischen Mitgliedstaaten und Drittländern – auch durch digitale Überwachung – auf, dafür zu sorgen, dass diese Dienste und deren Tätigkeiten einer umfassenden demokratischen Kontrolle im Rahmen einer angemessenen internen, exekutiven, justiziellen und unabhängigen parlamentarischen Kontrolle unterliegen;

30. betont, dass die Grundsätze der sozialen Verantwortung von Unternehmen und den Menschenrechten entsprechende Gestaltungsnormen („Human Rights by Design“), also technologische Lösungen und Innovationen, die dem Schutz der Menschenrechte Rechnung tragen, im EU-Recht niedergelegt werden sollten, damit dafür gesorgt ist, dass Internetdiensteanbieter (Internet Service Providers – ISP), Software-Entwickler, Hersteller von Hardware, soziale Netzwerkdienste/Medien, Mobilfunkbetreiber und andere die Menschenrechte der Nutzer weltweit berücksichtigen;

31. fordert die EU auf, für mehr Transparenz zu sorgen, was die Beziehung zwischen Mobilfunkbetreibern oder ISP und Regierungen angeht, und dies in ihren Beziehungen mit Drittländern einzufordern, indem die Anforderung aufgestellt wird, dass Mobilfunkbetreiber und ISP jährlich detaillierte Transparenzberichte veröffentlichen, einschließlich Berichten über Maßnahmen, die von staatlichen Stellen auferlegt werden, sowie über die finanziellen Beziehungen zwischen öffentlichen Stellen und Mobilfunkbetreibern/ISP;

32. erinnert die Wirtschaftsakteure an ihre Verantwortung, was die Achtung der Menschenrechte im Rahmen ihrer globalen Tätigkeiten angeht, und zwar ganz abgesehen davon, wo sich die entsprechenden Nutzer befinden sowie davon, ob der jeweilige Staat seinen eigenen Verpflichtungen in Bezug auf die Menschenrechte nachkommt; fordert die IKT-Unternehmen, insbesondere jene, die in der EU ansässig sind, auf, die Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte umzusetzen, unter anderem durch die Festlegung von Vorschriften über die Sorgfaltspflicht und von Vorsichtsmaßnahmen im Sinne des Risikomanagements sowie durch die Schaffung wirksamer Abhilfemaßnahmen für Fälle, in denen ihre Tätigkeiten zu Menschenrechtsverletzungen geführt oder beigetragen haben;

33. betont, dass die EU die Vorschriften und Sanktionen in Bezug auf IKT wirksamer umsetzen und ihre Einhaltung bzw. Auferlegung wirksamer überwachen muss und dabei auch Generalklauseln zur Anwendung kommen sollten, damit alle Parteien, einschließlich der Mitgliedstaaten, den Rechtsvorschriften Rechnung tragen und einheitliche Bedingungen gewahrt bleiben;

34. betont, dass die Achtung der Grundrechte ein wesentliches Element einer erfolgreichen Politik zur Bekämpfung des Terrorismus, einschließlich der Nutzung von Technologien zur digitalen Überwachung, darstellt;

35. begrüßt den Beschluss, der auf der Plenartagung des Wassenaar-Abkommens im Dezember 2013 über Ausfuhrkontrollen in Bezug auf Instrumente zur Überwachung, Strafverfolgung und Gewinnung nachrichtendienstlicher Erkenntnisse sowie Netzwerküberwachungssysteme getroffen wurde; erinnert daran, dass die Rechtsvorschriften der EU über Güter mit doppeltem Verwendungszweck, namentlich die EU-Verordnung über Güter mit doppeltem Verwendungszweck, sehr unvollständig sind, was wirksame, systematische Kontrollen der Ausfuhren schädlicher IKT-Technologien in undemokratische Länder angeht;

36. fordert die Kommission im Zusammenhang mit der anstehenden Überprüfung und Neugestaltung der Politik in Bezug auf Güter mit doppeltem Verwendungszweck nachdrücklich auf, rasch einen Vorschlag zu intelligenten, wirksamen Maßnahmen zur Beschränkung und Regelung der Ausfuhr zu kommerziellen Zwecken von Dienstleistungen für die Implementierung und Nutzung sogenannter Güter mit doppeltem Verwendungszweck vorzulegen, in dem auf die potenziell schädliche Ausfuhr von IKT-Produkten und -Dienstleistungen in Drittländer eingegangen wird, wie es in der Gemeinsamen Erklärung des Europäischen Parlaments, des Rates und der Kommission vom April 2014 vereinbart wurde; fordert die Kommission auf, wirksame Schutzvorkehrungen zu treffen, damit die Forschung, einschließlich der wissenschaftlichen Forschung und der Forschung in Bezug auf IT-Sicherheit, durch diese Ausfuhrkontrollen keinen Schaden nimmt;

37. betont, dass die Kommission in der Lage sein sollte, Unternehmen, denen unklar ist, ob sie eine Ausfuhrgenehmigung beantragen sollten, zeitnah aktuelle, korrekte Informationen über die Rechtmäßigkeit bzw. die potenziell schädlichen Auswirkungen möglicher Geschäfte zu übermitteln;

38. fordert die Kommission auf, Vorschläge für eine Prüfung der Frage vorzulegen, wie die in der EU geltenden Normen für IKT genutzt werden könnten, um potenziell schädlichen Auswirkungen der Ausfuhr solcher Technologien oder anderer Dienstleistungen in Drittländer, in denen Konzepte wie die „rechtmäßige

Überwachung“ nicht jenen der Europäischen Union entsprechen oder die beispielsweise eine schlechte Bilanz aufweisen, was die Menschenrechte angeht, oder in denen keine Rechtsstaatlichkeit existiert, entgegenzuwirken;

39. bekräftigt, dass die Normen der EU, insbesondere die Charta der Grundrechte der EU, bei der Bewertung von Vorfällen, bei denen Güter mit doppeltem Verwendungszweck so eingesetzt werden, dass es möglicherweise zu einer Beschneidung der Menschenrechte kommt, maßgeblich sein sollten;

40. fordert, dass Maßnahmen zur Regulierung des Verkaufs sogenannter Zero-Day-Exploits und von Sicherheitslücken ausgearbeitet werden, damit diese nicht für Cyber-Angriffe oder für den unbefugten Zugang zu Geräten und somit für Menschenrechtsverletzungen genutzt werden können, wobei sich eine derartige Regulierung allerdings nicht bedeutsam auf die akademische oder anderweitig angemessene Forschung im Bereich Sicherheit auswirken darf;

41. bedauert, dass bestimmte europäische und internationale Unternehmen, die in der EU tätig sind und mit Gütern mit doppeltem Verwendungszweck handeln, die potenziell die Wahrung der Menschenrechte beeinträchtigen, mit Regimen Geschäfte machen, deren Vorgehen die Menschenrechte verletzt;

42. fordert die Kommission auf, Unternehmen, die an solchen Tätigkeiten beteiligt sind, öffentlich aus den Verfahren des Beschaffungswesens der EU auszuschließen und an sie keine Mittel für Forschung und Entwicklung und auch keine anderen Finanzhilfen zu vergeben;

43. fordert die Kommission auf, Menschenrechtsaspekten bei den Verfahren des Beschaffungswesens für technologische Ausrüstung besondere Aufmerksamkeit zu widmen, und zwar insbesondere in Ländern, deren Vorgehensweise in diesem Bereich unzuverlässig ist;

44. fordert die Kommission und den Rat auf, das offene Internet, Entscheidungsverfahren unter Einbeziehung verschiedener Interessenträger, Netzneutralität, die digitalen Freiheiten sowie Datenschutzgarantien in Drittländern über Foren für die Verwaltung des Internets aktiv zu verteidigen;

45. verurteilt es, dass Verschlüsselungsprotokolle und -produkte geschwächt und konterkariert werden, insbesondere durch Nachrichtendienste, die verschlüsselte Kommunikationsprozesse ausspähen möchten;

46. warnt vor einer Privatisierung der Strafverfolgung durch Internetunternehmen und ISP;

47. fordert, dass geklärt wird, welche Normen und Standards Privatakteure bei der Entwicklung ihrer Systeme nutzen;

48. erinnert daran, dass unbedingt der Kontext bewertet werden muss, in dem Technologien genutzt werden, damit deren Auswirkungen auf die Menschenrechte umfassend eingeschätzt werden können;

49. fordert ausdrücklich, dass Instrumente gefördert werden, die es ermöglichen, das Internet anonym und/oder mittels Pseudonym zu nutzen, und dass die einseitige Ansicht in Frage gestellt wird, dass derartige Instrumente zwar für kriminelle Zwecke, allerdings nicht auch im Hinblick darauf genutzt werden könnten, Menschenrechtsverteidiger

außerhalb und innerhalb der EU zu stärken;

50. fordert den Rat, die Kommission und den EAD auf, intelligente, wirksame Maßnahmen zur Regulierung der Ausfuhr von Gütern mit doppeltem Verwendungszweck zu treffen und dabei potenziell schädlichen Ausfuhren von IKT-Produkten und -Dienstleistungen auf internationaler Ebene und im Rahmen multilateraler Ausfuhrkontrollvorschriften und anderer internationaler Gremien Rechnung zu tragen;

51. betont, dass jegliche Änderungen der Vorschriften, die auf eine Verbesserung der Wirksamkeit der Ausfuhrkontrollen für immaterielle Technologietransfers abzielen, nicht zu einer Beeinträchtigung der rechtmäßigen Forschung und des Zugangs zu Informationen sowie des Informationsaustauschs führen dürfen, und dass jegliche potenziellen Maßnahmen, beispielsweise die Anwendung der allgemeinen Ausfuhrgenehmigungen der Union auf Güter mit doppeltem Verwendungszweck, für Einzelpersonen und KMU nicht abschreckend sein sollten;

52. fordert die Mitgliedstaaten auf, dafür zu sorgen, dass die bestehenden und künftigen Ausfuhrkontrollmaßnahmen nicht zu einer Einschränkung der Tätigkeiten rechtmäßig vorgehender Forscher im Bereich Sicherheit führen, und dass Ausfuhrkontrollen in gutem Glauben und nur in Bezug auf klar definierte Technologien ausgeführt werden, die für die Zwecke der Massenüberwachung und von Zensur, Stör-, Abhör- und Kontrollmaßnahmen sowie der Verfolgung und Ortung von Bürgern und deren Aktivitäten in (Mobil-)Telefonnetzwerken genutzt werden sollen;

53. erinnert daran, dass kabellose Ad-hoc-Netze ein großes Potenzial für die Bereitstellung von Hilfsnetzen in Gebieten bergen, wo es kein Internet gibt oder dieses blockiert wird, und dass dies der Förderung der Menschenrechte dienen kann;

54. fordert die Kommission auf, eine unabhängige Sachverständigengruppe einzurichten, die Folgenabschätzungen in Bezug auf die Menschenrechte durchführen kann, was die bestehenden Normen der EU für IKT angeht, wobei das Ziel darin bestehen sollte, Empfehlungen für Anpassungen vorzulegen, mit denen die Menschenrechte insbesondere infolge der Ausfuhr von Systemen besser geschützt würden;

55. erkennt an, dass die technologische Entwicklung eine Herausforderung für die Rechtssysteme darstellt, da diese entsprechend an neue Umstände angepasst werden müssen; betont, dass die gesetzgebenden Organe sich stärker mit Fragen im Zusammenhang mit der Digitalwirtschaft beschäftigen müssen;

56. fordert die Kommission auf, die Zivilgesellschaft und unabhängige Sachverständige, darunter auch Personen, die im Bereich Sicherheit forschen, in den Bereich IKT in Drittländern einzubeziehen, damit aktuelles Expertenwissen zur Verfügung steht und somit zukunftssichere politische Maßnahmen verabschiedet werden;

57. betont, dass unbeabsichtigte Auswirkungen verhindert werden müssen, beispielsweise eine Einschränkung in Bezug auf die oder eine abschreckende Wirkung auf die rechtmäßige wissenschaftliche oder anderweitige Forschung und die entsprechende Entwicklung, auf den Austausch von und den Zugang zu Informationen, auf die Erlangung von Kenntnissen im Bereich Sicherheit oder auf die Ausfuhr von Technologien, die der Erlangung der erforderlichen digitalen Kompetenzen und der Förderung der Wahrung der Menschenrechte dienen;

58. vertritt die Auffassung, dass bei der weltweiten Zusammenarbeit zwischen Regierungen und Privatakteuren im digitalen Umfeld – auch im Rahmen des Internet Governance Forums – für eine angemessene gegenseitige Kontrolle gesorgt sein muss und die demokratische und justizielle Kontrolle dabei nicht konterkariert werden darf;

59. stellt fest, dass Freiwilligkeit nicht ausreicht, sondern es verbindlicher Vorschriften bedarf, um Unternehmen zu veranlassen, die Menschenrechtsbilanz von Ländern zu berücksichtigen, bevor sie ihre Produkte in diese Länder verkaufen, und eine Folgenabschätzung dazu durchführen, welche Folgen ihre Technologien auf Menschenrechtsverteidiger und Regierungskritiker haben werden;

60. ist der Auffassung, dass die Ausfuhr von hochsensiblen Gütern geprüft werden muss, bevor sie die EU verlassen, und dass Sanktionen durchgesetzt werden müssen, wenn es zu Verstößen kommt;

61. fordert, das jeder Einzelperson das Recht auf Verschlüsselung gewährt wird und auch die nötigen Voraussetzungen geschaffen werden, damit eine Verschlüsselung vorgenommen werden kann; vertritt die Auffassung, dass die Kontrolle bei den Endnutzern liegen sollte, die allerdings auch über die Kompetenzen verfügen müssen, die für die Durchführung entsprechender Kontrollen vonnöten sind;

62. fordert die Einführung von Standards für die Ende-zu-Ende-Verschlüsselung als Selbstverständlichkeit bei allen Kommunikationsdiensten, damit es Regierungen, Nachrichtendiensten und Überwachungsorganen erschwert wird, Inhalte mitzulesen;

63. betont, dass die staatlichen Nachrichtendienste eine besondere Verantwortung dahingehend tragen, Vertrauen zu schaffen, und fordert, die Massenüberwachung zu beenden; ist der Auffassung, dass die Überwachung der europäischen Bürger durch in- und ausländische Nachrichtendienste angegangen und beendet werden muss;

64. lehnt den Verkauf und die Verbreitung von europäischer Überwachungstechnologie und europäischen Zensurwerkzeugen an autoritäre Regime, in denen keine Rechtsstaatlichkeit herrscht, ab;

65. fordert, dass die Möglichkeiten, Whistleblowern internationalen Schutz zu bieten, ausgebaut werden, und legt den Mitgliedstaaten nahe, Gesetze zu deren Schutz auf den Weg zu bringen;

66. fordert einen UN-Beauftragten für digitale Freiheiten und Datenschutz sowie den Ausbau des Arbeitsbereichs des EU-Beauftragten für Menschenrechte dahingehend, dass auch Technologie unter dem Menschenrechtsaspekt betrachtet wird;

67. fordert Maßnahmen, die gewährleisten, dass die Privatsphäre von Aktivisten, Journalisten und Bürgern überall auf der Welt geschützt wird und sie sich über das Internet vernetzen können;

68. besteht darauf, dass das Recht auf einen Internetzugang als Menschenrecht anerkannt wird, und fordert Maßnahmen zur Beseitigung der digitalen Kluft;

69. beauftragt seinen Präsidenten, diese Entschließung dem Rat, der Kommission, der Vizepräsidentin der Europäischen Kommission/Hohen Vertreterin der Union für Außen- und Sicherheitspolitik sowie dem EAD zu übermitteln.