EUROPÄISCHES PARLAMENT 2009 – 2014

Plenarsitzungsdokument

A7-0139/2014

21.2.2014

BERICHT

über das 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 (2013/2188(INI))

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

Berichterstatter: Claude Moraes

INHALT

Seite

ENTWURF EINER ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS 3

BEGRÜNDUNG.....53

ANHANG I: LISTE DER ARBEITSDOKUMENTE.....61

ANHANG II: LISTE DER ANHÖRUNGEN UND SACHVERSTÄNDIGEN 62

ANHANG III: LISTE DER SACHVERSTÄNDIGEN, DIE DIE TEILNAHME AN DEN ÖFFENTLICHEN ANHÖRUNGEN DES LIBE-UNTERSUCHUNGSAUSSCHUSSES ABGELEHNT HABEN.....71

ERGEBNIS DER SCHLUSSABSTIMMUNG IM AUSSCHUSS 73

ENTWURF EINER ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS

zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, den Überwachungsbehörden in mehreren Mitgliedstaaten und den entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und der transatlantischen Zusammenarbeit im Bereich Justiz und Inneres (2013/2188(INI))

Das Europäische Parlament,

– gestützt auf den Vertrag über die Europäische Union (EUV), insbesondere auf die Artikel 2, 3, 4, 5, 6, 7, 10, 11 und 21,

– unter Hinweis auf den Vertrag über die Arbeitsweise der Europäischen Union (AEUV), insbesondere Artikel 15, 16 und 218 und Titel V,

– gestützt auf das Protokoll Nr. 36 über die Übergangsbestimmungen, insbesondere Artikel 10, und auf die 50. Erklärung zu diesem Protokoll,

– unter Hinweis auf die Charta der Grundrechte der Europäischen Union, insbesondere auf die Artikel 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 und 52,

– unter Hinweis auf die Europäische Menschenrechtskonvention, insbesondere Artikel 6, 8, 9, 10 und 13 und die dazugehörigen Protokolle,

– unter Hinweis auf die Allgemeine Erklärung der Menschenrechte, insbesondere Artikel 7, 8, 10,11,12 und 14[1],

– unter Hinweis auf den Internationalen Pakt über bürgerliche und politische Rechte, insbesondere Artikel 14, 17, 18 und 19,

– unter Hinweis auf das Übereinkommen des Europarats Nr. 108 zum Datenschutz und das Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten über Kontrollstellen und grenzüberschreitenden Datenverkehr vom 8. November 2001 (ETS Nr. 181),

– in Kenntnis des Wiener Übereinkommens über diplomatische Beziehungen, insbesondere der Artikel 24, 27 und 40,

– unter Hinweis auf das Übereinkommen des Europarats zur Cyberkriminalität (ETS Nr. 185),

– unter Hinweis auf den am 17. Mai 2010 veröffentlichten Bericht des VN-Sonderberichterstatters über die Förderung und den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des Terrorismus[2],

[1] http://www.un.org/en/documents/udhr/
[2] http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/134/10/PDF/G1214710.pdf?OpenElement

– unter Hinweis auf den am 17. April 2013 veröffentlichten Bericht des VN-Sonderberichterstatters über die Förderung und den Schutz des Rechts auf freie Meinungsäußerung[1],

– unter Hinweis auf die am 11. Juli 2002 vom Ministerausschuss des Europarats angenommenen Leitlinien für Menschenrechte und den Kampf gegen den Terrorismus,

– unter Hinweis auf die Brüsseler Erklärung vom 1. Oktober 2010, die auf der 6. Konferenz der Parlamentsausschüsse zur Kontrolle der Nachrichten- und Sicherheitsdienste der europäischen Mitgliedstaaten angenommen wurde,

– unter Hinweis auf die Entschließung 1954 (2013) der Parlamentarischen Versammlung des Europarates betreffend die nationale Sicherheit und den Zugang zu Informationen,

– unter Hinweis auf den am 11. Juni 2007 von der Venedig-Kommission angenommenen Bericht über die demokratische Aufsicht der Sicherheitsdienste[2] sowie unter Hinweis darauf, dass die im Frühjahr 2014 anstehende Aktualisierung dieses Berichts mit regem Interesse erwartet wird,

– unter Hinweis auf die Aussagen der Vertreter der Überwachungsausschüsse für die Geheimdienste von Belgien, den Niederlanden, Dänemark und Norwegen,

– unter Hinweis auf die bei den französischen[3], polnischen und britischen[4] Gerichten sowie beim Europäischen Gerichtshof für Menschenrechte[5] eingegangenen Rechtssachen in Zusammenhang mit Systemen zur Massenüberwachung,

– unter Hinweis auf das gemäß Artikel 34 des Vertrags über die Europäische Union durch den Rat erstellte Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, insbesondere Titel III[6],

– unter Hinweis auf die Entscheidung 520/2000 der Kommission vom 26. Juli 2000 über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA,

– unter Hinweis auf die Bewertungsberichte der Kommission vom 13. Februar 2002 (SEC(2002)0196) und vom 20. Oktober 2004 (SEC(2004)1323) zu der Umsetzung der Grundsätze des „sicheren Hafens" zum Datenschutz,

---

[1] http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
[2] http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx
[3] La Fédération Internationale des Ligues des Droits de l'Homme und La Ligue française pour la défense des droits de l'Homme et du Citoyen gegen X; X; Tribunal de Grande Instance von Paris.
[4] Fälle von Privacy International und Liberty beim Investigatory Powers Tribunal.
[5] Gemeinsamer Antrag gemäß Artikel 34 von Big Brother Watch, Open Rights Group, English Pen, Dr. Constanze Kurz (Antragsteller) - v - Vereinigtes Königreich (Beklagter).
[6] ABl. C 197 vom 12.7.2000, S. 1.

– in Kenntnis der Mitteilung der Kommission vom 27. November 2013 (COM(2013)0847) über das Funktionieren des sicheren Hafens aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen und der Mitteilung der Kommission vom 27. November 2013 (COM(2013)0846) über die Wiederherstellung des Vertrauens in den Datenfluss zwischen der EU und den USA,

– unter Hinweis auf seine Entschließung vom 5. Juli 2000 zu dem Entwurf einer Entscheidung der Kommission über die Angemessenheit der US-Grundsätze des Sicheren Hafens und diesbezügliche häufig gestellte Fragen (FAQ), vorgelegt vom Handelsministerium der USA, in der die Meinung vertreten wird, dass die Angemessenheit des Systems nicht bestätigt werden konnte[1], und auf die Stellungnahmen der Artikel-29-Arbeitsgruppe vom 16. Mai 2000[2], insbesondere Stellungnahme 4/2000,

– unter Hinweis auf die Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften (PNR-Abkommen) von 2004, 2007[3] und 2012[4],

– unter Hinweis auf die Gemeinsame Überprüfung der Durchführung des Abkommens zwischen der EU und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security[5], die gemeinsam mit dem Bericht der Kommission an das Europäische Parlament und den Rat über die gemeinsame Überprüfung vorgelegt wurde (COM(2013)0844),

– unter Hinweis auf die Stellungnahme von Generalanwalt Cruz Villalón, in der dieser folgerte, dass die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, mit Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union insgesamt unvereinbar ist, und dass Artikel 6 der Richtlinie mit Artikel 7 und Artikel 52 Absatz 1 der Charta[6] unvereinbar ist,

– unter Hinweis auf den Beschluss 2010/412/EU des Rates vom 13. Juli 2010 über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (TFTP)[7] und auf die dazugehörigen Erklärungen der Kommission und des Rates,

– unter Hinweis auf das Abkommen zwischen der Europäischen Union und den

---

[1] ABl. C 121 vom 24.4.2001, S. 152.
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf
[3] ABl. L 204 vom 4.8.2007, S. 18.
[4] ABl. L 215 vom 11.8.2012, S. 5.
[5] SEC(2013) 0630 vom 27.11.2013.
[6] Schlussanträge des Generalanwalts Cruz Villalón vom 12. Dezember 2013 in der Rechtssache C-293/12.
[7] ABl. L 195 vom 27.7.2010, S. 3.

Vereinigten Staaten von Amerika über Rechtshilfe[1],

– unter Hinweis auf die laufenden Verhandlungen über ein Rahmenabkommen zwischen der EU und den USA über den Schutz personenbezogener Daten, die zum Zweck der Verhinderung, Ermittlung, Aufdeckung und Verfolgung von Straftaten einschließlich des Terrorismus im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (das „Rahmenabkommen“) übermittelt und verarbeitet werden,

– unter Hinweis auf die Verordnung (EG) Nr. 2271/96 des Rates vom 22. November 1996 zum Schutz vor den Auswirkungen der extraterritorialen Anwendung von einem Drittland erlassener Rechtsakte sowie von darauf beruhenden oder sich daraus ergebenden Maßnahmen[2],

– unter Hinweis auf die Erklärung des Präsidenten der Föderativen Republik Brasilien bei der Eröffnung der 68. Sitzung der UN-Generalversammlung am 24. September 2013 und der Arbeit des durch den Bundessenat Brasiliens eingesetzten Parlamentarischen Untersuchungsausschusses zu Spionage,

– unter Hinweis auf den „USA-PATRIOT Act“, der von Präsident George W. Bush am 26. Oktober 2001 unterzeichnet wurde,

– unter Hinweis auf den „Foreign Intelligence Surveillance Act“ (FISA) von 1978 und den „FISA Amendments Act“ von 2008,

– unter Hinweis auf die vom US-Präsidenten 1981 vorgelegte und 2008 geänderte Ausführungsverordnung Nr. 12333,

– in Kenntnis der „US Presidential Policy Directive on Signals Intelligence Activities, PPD-28“ (Grundsatzrichtlinie des US-Präsidenten über signalerfassende Aufklärung), die am 17. Januar 2014 von Präsident Barack Obama erlassen wurde,

– unter Hinweis auf derzeit im US-Kongress zur Debatte stehende Legislativvorschläge, darunter den Entwurf des „US Freedom Act“, den Entwurf des „Oversight and Surveillance Reform Act“ und andere,

– unter Hinweis auf die von der Stelle zur Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten (Privacy and Civil Liberties Oversight Board), dem Nationalen Sicherheitsrat der USA und der Arbeitsgruppe des Präsidenten zu Nachrichtendienst und Kommunikationstechnik durchgeführten Überprüfungen, insbesondere auf den Bericht der letzteren vom 12. Dezember 2013 mit dem Titel „Liberty and Security in a Changing World“ (Freiheit und Sicherheit in einer sich verändernden Welt),

– unter Hinweis auf das Urteil des „United States District Court for the District of Columbia“ in der Rechtssache Klayman et al. v Obama et al., Civil Action Nr. 13-0851 vom 16. Dezember 2013 und das Urteil des „United States District Court for the

[1] ABl. L 181 vom 19.7.2003, S. 34.
[2] ABl. L 309 vom 29.11.1996, S. 1.

Southern District of New York“ in der Rechtssache ACLU et al. v James R., Clapper u.a., Civil Action Nr. 13-3994 vom 11. Juni 2013,

– unter Hinweis auf den Bericht über die Ergebnisse der EU-Ko-Vorsitzenden der Ad-hoc-Arbeitsgruppe der EU und der USA zum Datenschutz vom 27. November 2013[1],

– unter Hinweis auf seine Entschließungen vom 5. September 2001 und 7. November 2002 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon),

– unter Hinweis auf seine Entschließung vom 21. Mai 2013 über die EU-Charta: Normensetzung für die Freiheit der Medien in der EU[2],

– unter Hinweis auf seine Entschließung vom 4. Juli 2013 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, den Überwachungsbehörden in mehreren Mitgliedstaaten und den entsprechenden Auswirkungen auf die Privatsphäre der EU-Bürger, mit der sein Ausschuss für bürgerliche Freiheiten, Justiz und Inneres beauftragt wurde, diesen Sachverhalt eingehend zu untersuchen[3],

– unter Hinweis auf das Arbeitsdokument 1 über die Überwachungsprogramme der USA und der EU und ihre Auswirkungen auf die Grundrechte der EU-Bürger,

– unter Hinweis auf das Arbeitsdokument 3 über das Verhältnis zwischen der Überwachungstätigkeit in der EU sowie in den USA und den Datenschutzbestimmungen der Europäischen Union,

– unter Hinweis auf das Arbeitsdokument 4 zu der US-Überwachung von EU-Daten und möglichen Auswirkungen auf transatlantische Abkommen und Zusammenarbeit,

– unter Hinweis auf das Arbeitsdokument 5 über die demokratische Kontrolle von Nachrichtendiensten der Mitgliedstaaten und Nachrichtendiensten der EU,

– unter Hinweis auf seine Entschließung vom 23. Oktober 2013 zu organisiertem Verbrechen, Korruption und Geldwäsche: Empfohlene Maßnahmen und Initiativen[4],

– unter Hinweis auf seine Entschließung vom 23. Oktober 2013 zur Aussetzung des TFTP-Abkommens infolge der Überwachungsmaßnahmen der NSA[5],

– unter Hinweis auf seine Entschließung vom 10. Dezember 2013 zur Freisetzung des Cloud-Computing-Potenzials in Europa[6],

– in Kenntnis der Interinstitutionellen Vereinbarung zwischen dem Europäischen

---

[1] Ratsdokument 16987/13.
[2] Angenommene Texte, P7_TA(2013)0203.
[3] Angenommene Texte, P7_TA(2013)0322.
[4] Angenommene Texte, P7_TA(2013)0444.
[5] Angenommene Texte, P7_TA(2013)0449.
[6] Angenommene Texte, P7_TA(2013)0535.

Parlament und dem Rat über die Übermittlung an und die Bearbeitung durch das Europäische Parlament von im Besitz des Rates befindlichen Verschlusssachen in Bezug auf Angelegenheiten, die nicht unter die Gemeinsame Außen- und Sicherheitspolitik fallen[1],

– gestützt auf Anhang VIII seiner Geschäftsordnung,

– gestützt auf Artikel 48 seiner Geschäftsordnung,

– in Kenntnis des Berichts des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (A7-0139/2014),

Auswirkungen von Massenüberwachung

A. in der Erwägung, dass Datenschutz und Privatsphäre Grundrechte sind; in der Erwägung, dass Sicherheitsmaßnahmen, einschließlich Maßnahmen zur Bekämpfung des Terrorismus, unter Wahrung der Rechtsstaatlichkeit erfolgen und aus den Grundrechten erwachsenden Verpflichtungen, wozu auch die zur Privatsphäre und zum Datenschutz gehören, unterliegen müssen;

B. in der Erwägung, dass die Beziehungen zwischen Europa und den Vereinigten Staaten von Amerika auf dem Geist und den Grundsätzen von Demokratie, Rechtsstaatlichkeit, Freiheit, Gerechtigkeit und Solidarität beruhen;

C. in der Erwägung, dass die Zusammenarbeit zwischen den Vereinigten Staaten und der Europäischen Union und ihren Mitgliedstaaten bei der Bekämpfung des Terrorismus für den Schutz und die Sicherheit beider Partner weiterhin von grundlegender Bedeutung ist;

D. in der Erwägung, dass gegenseitiges Vertrauen und Verständnis Schlüsselfaktoren im transatlantischen Dialog und in der Partnerschaft darstellen;

E. in der Erwägung, dass nach dem 11. September 2001 die Bekämpfung von Terrorismus zu einer der höchsten Prioritäten der meisten Regierungen geworden ist; in der Erwägung, dass führende Politiker infolge der Enthüllungen aufgrund von Dokumenten, die der ehemalige Mitarbeiter der NSA Edward Snowden offengelegt hat, verpflichtet sind, den Herausforderungen bei der Aufsicht und Kontrolle von Geheimdiensten bei Überwachungstätigkeiten und bei der Beurteilung der Auswirkungen ihrer Tätigkeiten auf die Grundrechte und die Rechtsstaatlichkeit in einer demokratischen Gesellschaft zu begegnen;

F. in der Erwägung, dass die Enthüllungen seit Juni 2013 in der EU zahlreiche Bedenken hinsichtlich folgender Punkte ausgelöst haben:

- das sowohl in den Vereinigten Staaten als auch in den EU-Mitgliedstaaten enthüllte Ausmaß an Überwachungssystemen;
- die Verletzung von EU-Bestimmungen, Grundrechten und

[1] ABl. C 353 E vom 3.12.2013, S. 156.

Datenschutzstandards;

- das Maß an Vertrauen zwischen den transatlantischen Partnern EU und USA;
- das Ausmaß der Zusammenarbeit mit und der Beteiligung an Überwachungsprogrammen der USA oder gleichwertigen Programmen auf nationaler Ebene durch bestimmte EU-Mitgliedstaaten, das von den Medien enthüllt wurde;
- das Fehlen von Kontrolle und wirksamer Aufsicht durch die politischen Behörden der USA und bestimmte EU-Mitgliedstaaten über ihre Nachrichtendienste;
- die Möglichkeit, dass diese Massenüberwachung für andere Zwecke als die der nationalen Sicherheit und der Bekämpfung des Terrorismus im eigentlichen Sinn genutzt wird, etwa für Wirtschafts- und Industriespionage oder zur Profilerstellung aus politischen Gründen;
- die Beeinträchtigung der Pressefreiheit und der Kommunikation mit Angehörigen der Berufe mit Vertraulichkeitsprivilegien wie Rechtsanwälten und Ärzten;
- die jeweiligen Rollen und der Grad der Beteiligung von Nachrichtendiensten und privaten IT- und Telekommunikationsunternehmen;
- die zunehmend verschwimmenden Grenzen zwischen Strafverfolgung und nachrichtendienstlichen Tätigkeiten, wodurch jeder Bürger als Verdächtiger behandelt und Überwachungsobjekt wird;
- die Bedrohung der Privatsphäre in einem digitalen Zeitalter;

G. in der Erwägung, dass das beispiellose Ausmaß der enthüllten Spionage einer umfassenden Untersuchung durch die US-Behörden, die europäischen Institutionen und die Regierungen, nationalen Parlamente und Justizbehörden der Mitgliedstaaten bedarf;

H. in der Erwägung, dass die US-Behörden zwar einige der offengelegten Informationen bestreiten, die überwiegende Mehrheit allerdings nicht angefochten haben; in der Erwägung, dass sich die öffentliche Debatte in den USA und in bestimmten EU-Mitgliedstaaten in großem Umfang entwickelt hat; in der Erwägung, dass die entsprechende Regierungen und Parlamente der EU zu oft schweigen und es versäumen, Untersuchungen einzuleiten;

I. in der Erwägung, dass Präsident Barack Obama kürzlich eine Reform der NSA und ihrer Überwachungsprogramme angekündigt hat;

J. in der Erwägung, dass das Europäische Parlament im Gegensatz zu dem Vorgehen sowohl anderer EU-Institutionen als auch bestimmter EU-Mitgliedstaaten seine Verpflichtung sehr ernst genommen hat, die Enthüllungen über die willkürlichen Verfahren der Massenüberwachung von EU-Bürgerinnen und -Bürgern aufzuklären, und mittels seiner Entschließung vom 4. Juli 2013 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, den

Überwachungsbehörden in mehreren Mitgliedstaaten und den entsprechenden Auswirkungen auf die Privatsphäre der EU-Bürger seinen Ausschuss für bürgerliche Freiheiten, Justiz und Inneres mit der Durchführung einer eingehenden Untersuchung beauftragt hat;

K. in der Erwägung, dass es die Pflicht der europäischen Institutionen ist, sicherzustellen, dass EU-Recht vollständig zum Nutzen der europäischen Bürgerinnen und Bürger umgesetzt wird und dass die Rechtsgültigkeit der EU-Verträge nicht durch eine bagatellisierende Inkaufnahme der extraterritorialen Auswirkungen der Aktivitäten oder Normen von Drittländern beeinträchtigt wird;

Entwicklungen in den USA hinsichtlich der Reform der Nachrichtendienste

L. in der Erwägung, dass der „District Court for the District of Columbia“ mit seinem Urteil vom 16. Dezember 2013 entschieden hat, dass die Sammelerhebung von Metadaten durch die NSA gegen die Vierte Änderung der Verfassung der USA[1] verstößt; in der Erwägung, dass der „District Court for the Southern District of New York“ in seinem Urteil vom 27. Dezember 2013 jedoch entschieden hat, dass diese Form der Erhebung rechtmäßig ist;

M. in der Erwägung, dass ein Beschluss des „District Court for the Eastern District of Michigan“ entschieden hat, dass in der Vierten Änderung die Angemessenheit aller Durchsuchungen, vorherige Durchsuchungsbefehle für jede angemessene Durchsuchung, Durchsuchungsbefehle auf Grundlage eines bereits bestehenden hinreichenden Verdachts sowie Sorgfalt in Bezug auf Personen, Orte und Dinge und die Zwischenschaltung eines neutralen Richters zwischen den Vollstreckungsbeamten der Exekutive und den Bürgern vorgeschrieben sind[2];

N. in der Erwägung, dass die Arbeitsgruppe des Präsidenten zu Nachrichtendienst und Kommunikationstechnik in ihrem Bericht vom 12. Dezember 2013 46 Empfehlungen an den Präsidenten der Vereinigten Staaten richtet; in der Erwägung, dass in diesen Empfehlungen die Notwendigkeit betont wird, nationale Sicherheit und persönliche Privatsphäre und bürgerliche Freiheiten gleichzeitig zu schützen; in der Erwägung, dass die US-Regierung in dieser Hinsicht aufgefordert wird, die Sammelerfassung der Telefon-Datensätze von US-Bürgern gemäß § 215 des „USA-PATRIOT Act“ so bald wie möglich einzustellen, eine umfassende Überarbeitung des Rechtsrahmens von NSA und US-Nachrichtendiensten zur Sicherstellung der Einhaltung des Rechts auf Privatsphäre vorzunehmen, die Sabotage kommerzieller Softwareprodukte (Backdoors und Malware) zu beenden, den Einsatz von Verschlüsselung insbesondere bei der Datenübertragung zu erhöhen und Bemühungen zur Entwicklung von Verschlüsselungsstandards nicht zu untergraben, einen Verfechter des öffentlichen Interesses zur Verteidigung der Privatsphäre und der bürgerlichen Freiheiten vor dem „Foreign Intelligence Surveillance Court“ einzusetzen, dem „Privacy and Civil Liberties Oversight Board“ die Befugnis zu übertragen, nachrichtendienstliche Aktivitäten zu beaufsichtigen, die zu den Zwecken ausländischer Geheimdienste und nicht nur für die Terrorismusbekämpfung durchgeführt werden, und die Beschwerden

[1] Klayman et al. v Obama et al., Civil Action No 13-0851, 16. Dezember 2013.
[2] ACLU v. NSA Nr. 06-CV-10204, 17. August 2006.

von Informanten entgegenzunehmen, für den Erhalt elektronischer Kommunikation bilaterale Rechtshilfeverträge einzusetzen und Überwachung nicht dazu zu verwenden, Betriebs- oder Handelsgeheimnisse zu stehlen;

O. in der Erwägung, dass aus einem offenen Memorandum, das ehemalige Funktionsträger der NSA und die „Veteran Intelligence Professionals for Sanity“ (VIPS) am 7. Januar 2014 an Präsident Barack Obama übergeben haben[1], hervorgeht, dass die Massenerhebung von Daten die Fähigkeit zur Verhinderung von Terroranschlägen nicht verbessert; in der Erwägung, dass die Verfasser hervorheben, dass die von der NSA durchgeführte Überwachung in keinem Fall zur Verhinderung eines Anschlags beigetragen hat und dass Milliarden Dollar für Programme ausgegeben wurden, die weniger wirksam sind und weitaus stärker in die Privatsphäre der Bürgerinnen und Bürger eingreifen als eine hauseigene Technologie namens THINTHREAD aus dem Jahr 2001;

P. in der Erwägung, dass in den Empfehlungen an den US-Präsidenten betreffend nachrichtendienstliche Aktivitäten gegen Nicht-US-Bürger gemäß § 702 FISA das grundlegende Prinzip der Achtung der Privatsphäre und der Menschenwürde anerkannt wird, wie es in Artikel 12 der Allgemeinen Erklärung der Menschenrechte und in Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte verankert ist; in der Erwägung, dass nicht empfohlen wird, Nicht-US-Bürgern die gleichen Rechte und den gleichen Schutz wie US-Bürgern zu gewähren;

Q. in der Erwägung, dass US-Präsident Barack Obama in seiner Grundsatzrichtlinie über signalerfassende Aufklärung vom 17. Januar 2014 feststellte, dass die elektronische Massenüberwachung für die Vereinigten Staaten ein notwendiges Mittel sei, um die nationale Sicherheit zu verteidigen, die Bürgerinnen und Bürger des eigenen Landes und seiner Verbündeten und Partner zu schützen und die außenpolitischen Interessen der USA zu fördern; in der Erwägung, dass diese Grundsatzrichtlinie bestimmte Prinzipien betreffend die Sammelerhebung, die Verwendung und die Weitergabe von Signalaufklärung enthält und bestimmte Sicherheitsgarantien auf Nicht-US-Bürger ausweitet und damit zum Teil eine gleichwertige Behandlung im Vergleich zu US-Bürgern vorsieht, einschließlich Sicherheiten für die personenbezogenen Informationen aller Menschen ungeachtet ihrer Staatsangehörigkeit oder ihres Wohnsitzes; in der Erwägung, dass Präsident Barack Obama jedoch keine konkreten Vorschläge, insbesondere zum Verbot der Massenüberwachung und zur Einführung von gerichtlichen und behördlichen Rechtsbehelfen für Nicht-US-Bürger, gefordert hat;

Rechtsrahmen

Grundrechte

R. in der Erwägung, dass der Bericht über die Ergebnisse der EU-Ko-Vorsitzenden der Ad-hoc-Arbeitsgruppe der EU und der USA zum Datenschutz zwar einen Überblick über die rechtliche Situation in den USA gibt, es mit ihm jedoch nicht gelungen ist, die Fakten zu Überwachungsprogrammen der USA zu ermitteln; in der Erwägung, dass es

[1] http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong.

zu der sogenannten Arbeitsgruppe des „zweiten Weges“, unter der die Mitgliedstaaten bilateral mit US-Behörden Fragen im Zusammenhang mit nationaler Sicherheit erörtern, keine Informationen gibt;

S. in der Erwägung, dass Grundrechte, insbesondere freie Meinungsäußerung, Pressefreiheit, Gedanken-, Gewissens-, Religions- und Versammlungsfreiheit, Schutz der Privatsphäre, Datenschutz sowie das Recht auf einen wirksamen Rechtsbehelf, auf Unschuldsvermutung, auf ein faires Verfahren und Nichtdiskriminierung, wie sie in der Charta der Grundrechte der Europäischen Union und in der Europäischen Menschenrechtskonvention verankert sind, die Eckpfeiler der Demokratie darstellen; in der Erwägung, dass die Massenüberwachung von Menschen mit diesen Eckpfeilern unvereinbar ist;

T. in der Erwägung, dass die Rechtsvorschriften in allen Mitgliedstaaten vor der Offenlegung von Informationen schützen, die vertraulich zwischen Rechtsanwalt und Mandant behandelt wurden, und dass dieser Grundsatz vom Europäischen Gerichtshof bestätigt worden ist[1];

U. in der Erwägung, dass das Parlament in seiner Entschließung zu organisiertem Verbrechen, Korruption und Geldwäsche vom 23. Oktober 2013 die Kommission aufgefordert hat, einen Gesetzesvorschlag vorzulegen, der ein wirksames und umfassendes europäisches Schutzprogramm für Informanten vorsieht, um die finanziellen Interessen der EU zu schützen, und ferner eine Untersuchung durchzuführen, ob eine solche künftige Rechtsvorschrift auch andere Zuständigkeitsbereiche der Union abdecken sollte;

Zuständigkeiten der Union im Bereich Sicherheit

V. in der Erwägung, dass nach Artikel 67 Absatz 3 AEUV die Union „darauf hinwirkt, ein hohes Maß an Sicherheit zu gewährleisten“; in der Erwägung, dass die EU gemäß den Bestimmungen des Vertrags (insbesondere Artikel 4 Absatz 2 EUV, Artikel 72 AEUV und Artikel 73 AEUV) bestimmte Zuständigkeiten hinsichtlich der kollektiven äußeren Sicherheit der Union besitzt; in der Erwägung, dass die EU Zuständigkeiten hinsichtlich interner Sicherheit hat (Artikel 4 Buchstabe j AEUV) und diese wahrnimmt, indem sie zur Bekämpfung schwerer Straftaten und des Terrorismus Rechtsinstrumente festlegt und internationale Abkommen (PNR, TFTP) abschließt und indem sie eine Strategie für interne Sicherheit aufstellt und auf diesem Gebiet tätige Stellen einrichtet;

W. in der Erwägung, dass es den Mitgliedstaaten gemäß dem Vertrag über die Arbeitsweise der Europäischen Union freisteht, „untereinander und in eigener Verantwortung Formen der Zusammenarbeit und Koordinierung zwischen den zuständigen Dienststellen ihrer für den Schutz der nationalen Sicherheit verantwortlichen Verwaltungen einzurichten, die sie für geeignet halten“ (Artikel 73 AEUV);

[1] Urteil vom 18. Mai 1982 in der Rechtssache 155/79, AM and S Europe Limited gegen Kommission der Europäischen Gemeinschaften.

X. in der Erwägung, dass der Gerichtshof der Europäischen Union gemäß Artikel 276 AEUV „[b]ei der Ausübung seiner Befugnisse im Rahmen der Bestimmungen des Dritten Teils Titel V Kapitel 4 und 5 über den Raum der Freiheit, der Sicherheit und des Rechts […] nicht zuständig [ist] für die Überprüfung der Gültigkeit oder Verhältnismäßigkeit von Maßnahmen der Polizei oder anderer Strafverfolgungsbehörden eines Mitgliedstaats oder der Wahrnehmung der Zuständigkeiten der Mitgliedstaaten für die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der inneren Sicherheit“;

Y. in der Erwägung, dass sich die Begriffe „nationale Sicherheit“, „interne Sicherheit“, „interne Sicherheit der EU“ und „internationale Sicherheit“ überschneiden; in der Erwägung, dass das Wiener Übereinkommen über das Recht der Verträge, der Grundsatz loyaler Zusammenarbeit unter den Mitgliedstaaten und der Grundsatz der Auslegung von Ausnahmeregelungen der Menschenrechte auf eine einschränkende Auslegung des Begriffs der „nationalen Sicherheit“ hinweisen und verlangen, dass die Mitgliedstaaten es unterlassen, sich in die Zuständigkeiten der EU einzumischen;

Z. in der Erwägung, dass der Kommission durch die EU-Verträge die Rolle der „Hüterin der Verträge“ übertragen wird und ihr daher von Rechts wegen die Zuständigkeit obliegt, etwaige Verstöße gegen EU-Recht zu untersuchen;

AA. in der Erwägung, dass öffentliche oder nicht-öffentliche Stellen der Mitgliedstaaten, die im Bereich der nationalen Sicherheit tätig sind, gemäß Artikel 6 EUV, der sich auf die EU-Grundrechtecharta und die EMRK bezieht, auch die hierin verankerten Rechte einhalten müssen, sei es in Bezug auf ihre eigenen Bürgerinnen und Bürger oder die Bürgerinnen und Bürger anderer Staaten;

Extraterritorialität

AB. in der Erwägung, dass in den Situationen, die unter die Rechtsprechung der EU oder eines ihrer Mitgliedstaaten fallen, die extraterritoriale Anwendung seiner Gesetzgebung, Bestimmungen und anderer legislativer oder exekutiver Instrumente durch einen Drittstaat die geltende Rechtsordnung und Rechtsstaatlichkeit beeinträchtigen oder sogar internationales oder EU-Recht, einschließlich der Rechte natürlicher oder juristischer Personen, verletzen kann, abhängig von dem Ausmaß und dem erklärten oder tatsächlichen Zweck dieser Anwendung; in der Erwägung, dass es unter diesen Umständen notwendig ist, Maßnahmen auf Unionsebene zu ergreifen, um sicherzustellen, dass die in Artikel 2 EUV, der Charta der Grundrechte, der EMRK in Bezug auf die Grundrechte, Demokratie und Rechtsstaatlichkeit verankerten Werte der EU sowie die Rechte natürlicher oder juristischer Personen in der EU gemäß den abgeleiteten Rechtsvorschriften zur Anwendung dieser wesentlichen Grundsätze geachtet werden, beispielsweise indem die Auswirkungen der betreffenden ausländischen Gesetzgebung beseitigt, ausgeglichen oder blockiert werden oder ihnen auf andere Wese entgegengewirkt wird;

Internationale Datenübermittlungen

AC. in der Erwägung, dass sich durch die Übermittlung personenbezogener Daten zu Strafverfolgungszwecken durch Organe, Einrichtungen, Ämter und Stellen der EU

oder durch die Mitgliedstaaten an die USA ohne angemessene Sicherheitsgarantien und Schutzvorkehrungen für die Einhaltung der Grundrechte der EU-Bürger, insbesondere des Rechts auf Privatsphäre und auf den Schutz personenbezogener Daten, dieses Organ, diese Einrichtung, dieses Amt oder diese Stelle der EU oder dieser Mitgliedstaat gemäß Artikel 340 AEUV oder der ständigen Rechtsprechung des EuGH[1] schuldig an der Verletzung von EU-Recht macht – dies schließt die Verletzung der in der EU-Charta verankerten Grundrechte ein;

AD. in der Erwägung, dass die Übermittlung von Daten keinen geografischen Beschränkungen unterliegt und sich der EU-Gesetzgeber besonders im Zusammenhang mit der zunehmenden Globalisierung und weltweiten Kommunikation neuen Herausforderungen beim Schutz personenbezogener Daten und Kommunikation gegenübersieht; in der Erwägung, dass es daher von entscheidender Bedeutung ist, die rechtlichen Rahmenbedingungen für gemeinsame Normen zu fördern;

AE. in der Erwägung, dass die Massenerhebung von personenbezogenen Daten für gewerbliche Zwecke und zur Bekämpfung des Terrorismus und schwerer grenzüberschreitender Straftaten die Rechte der EU-Bürgerinnen und -Bürger auf den Schutz personenbezogener Daten und auf Privatsphäre gefährdet;

Übermittlung an die USA auf der Grundlage des „sicheren Hafens“

AF. in der Erwägung, dass mit dem Datenschutz-Rechtsrahmen der Vereinigten Staaten kein angemessenes Schutzniveau für EU-Bürger sichergestellt wird;

AG. in der Erwägung, dass die Kommission in ihrer Entscheidung 520/2000 die Angemessenheit des von den vom Handelsministerium der USA vorgelegten Grundsätzen des sicheren Hafens und der diesbezüglichen häufig gestellten Fragen (FAQ) gewährleisteten Schutzes personenbezogener Daten, die von der Union an dem sicheren Hafen beigetretene Unternehmen in den Vereinigten Staaten übermittelt werden, erklärt hat, um es den für die Datenverarbeitung Verantwortlichen in der EU zu ermöglichen, personenbezogene Daten an eine Stelle in den USA zu übermitteln;

AH. in der Erwägung, dass das Parlament in seiner Entschließung vom 5. Juli 2000 Zweifel und Bedenken an der Angemessenheit des sicheren Hafens geäußert und die Kommission aufgefordert hat, ihre Entscheidung vor dem Hintergrund von Erfahrungen und legislativer Entwicklungen zeitnah zu überprüfen;

AI. in der Erwägung, dass in dem Arbeitsdokument 4 des Parlaments zu der US-Überwachung von EU-Daten und möglichen Auswirkungen auf transatlantische Abkommen und Zusammenarbeit vom 12. Dezember 2013 der Berichterstatter Zweifel und Bedenken mit Blick auf die Angemessenheit des Systems des sicheren Hafens äußert und die Kommission auffordert, die Entscheidung über die Angemessenheit dieses Systems aufzuheben und neue gesetzliche Lösungen zu finden;

AJ. in der Erwägung, dass in der Entscheidung 520/2000 der Kommission vorgesehen ist,

[1] Siehe insbesondere Verbundene Rechtssachen C-6/90 und C-9/90, Francovich und andere gegen Italienische Republik, Urteil vom 28. Mai 1991.

dass die zuständigen Behörden in den Mitgliedstaaten ihre bestehenden Befugnisse ausüben können, um zum Schutz von Privatpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung an eine Organisation auszusetzen, die den Grundsätzen, die entsprechend den FAQ umgesetzt wurden, beigetreten ist, wenn eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze des sicheren Hafens verletzt werden, oder die fortgesetzte Datenübermittlung für die betroffenen Personen ein unmittelbares Risiko eines schweren Schadens bergen würde;

AK. in der Erwägung, dass in der Entscheidung 520/2000 der Kommission auch festgelegt wird, dass die Kommission, wenn es Hinweise darauf gibt, dass eine der für die Einhaltung der Grundsätze verantwortlichen Einrichtungen ihrer Aufgabe nicht wirkungsvoll nachkommt, das Handelsministerium der USA informiert und, wenn nötig, im Hinblick auf eine Aufhebung, Aussetzung oder Beschränkung des Geltungsbereichs der Entscheidung entsprechende Maßnahmen vorschlägt;

AL. in der Erwägung, dass die Kommission in ihren ersten beiden Berichten zu der Umsetzung des sicheren Hafens, die 2002 und 2004 veröffentlicht wurden, mehrere Mängel hinsichtlich der ordnungsgemäßen Umsetzung des sicheren Hafens ermittelt und an die US-Behörden eine Reihe von Empfehlungen gerichtet hat, um diese Mängel zu korrigieren;

AM. in der Erwägung, dass die Kommission in ihrem dritten Durchführungsbericht vom 27. November 2013, neun Jahre nach dem zweiten Bericht und ohne dass die in dem Bericht ermittelten Mängel korrigiert worden wären, weitere weitreichende Schwächen und Unzulänglichkeiten des sicheren Hafens festgestellt und daraus gefolgert hat, dass die derzeitige Umsetzung nicht aufrechterhalten werden könne; in der Erwägung, dass die Kommission betont hat, dass durch den weitreichenden Zugriff von US-Nachrichtendiensten auf Daten, die den USA durch Safe-Harbour-zertifizierte Stellen übermittelt wurden, ernsthafte Fragen nach dem Fortbestand des Datenschutzes von EU-Personen aufgeworfen werden; in der Erwägung, dass die Kommission 13 Empfehlungen an die US-Behörden gerichtet hat und bis Sommer 2014 zusammen mit den US-Behörden schnellstmöglich umzusetzende Abhilfemaßnahmen ermitteln will, um so die Grundlage für eine umfassende Überarbeitung der Funktionsweise der Grundsätze des sicheren Hafens zu legen;

AN. in der Erwägung, dass vom 28. bis 31. Oktober 2013 eine Delegation des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments in Washington D.C. mit dem US-Handelsministerium und der US-Handelskommission zusammentraf; in der Erwägung, dass das Handelsministerium das Bestehen von Organisationen anerkannt hat, die ihre Einhaltung der Grundsätze des sicheren Hafens selbst zertifiziert haben, dieser Status jedoch eindeutig nicht aktuell ist, das Unternehmen die Anforderungen an den sicheren Hafen also nicht erfüllt, obgleich es weiterhin personenbezogene Daten aus der EU erhält; in der Erwägung, dass die US-Handelskommission zugestanden hat, dass der sichere Hafen überarbeitet werden muss, um ihn zu verbessern, insbesondere hinsichtlich Beschwerden und alternativer Streitbeilegungsverfahren;

AO. in der Erwägung, dass die Grundsätze des sicheren Hafens „insoweit, als

Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss“ begrenzt werden können; in der Erwägung, dass eine Ausnahme von einem Grundrecht stets restriktiv ausgelegt und darauf beschränkt werden muss, was in einer demokratischen Gesellschaft notwendig und angemessen ist, und in der Erwägung, dass die Bedingungen und Garantien für die Legitimität dieser Einschränkung deutlich in der Gesetzgebung festgelegt sein müssen; in der Erwägung, dass der Anwendungsbereich einer solchen Ausnahme von den Vereinigten Staaten und der EU, speziell der Kommission, hätte geklärt werden sollen, um jegliche Auslegung oder Anwendung zu vermeiden, die unter anderem das Grundrecht auf Privatsphäre und Datenschutz im Grunde aufhebt; in der Erwägung, dass eine solche Ausnahme demzufolge nicht auf eine Art angewendet werden sollte, durch die der von der Charta der Grundrechte, der EMRK, vom EU-Datenschutzgesetz und von den Grundsätzen des sicheren Hafens gewährte Schutz beeinträchtigt oder aufgehoben wird; in der Erwägung, dass bei der Anwendung der Ausnahmeregelung aus Gründen der nationalen Sicherheit in jedem Fall Angaben zu dem dabei angewandten nationalen Recht erfolgen müssen;

AP. in der Erwägung, dass das transatlantische Vertrauen durch den groß angelegten Zugriff von US-Nachrichtendiensten ernsthaft erschüttert und das Vertrauen hinsichtlich US-Organisationen, die in der EU tätig sind, negativ beeinflusst worden ist; in der Erwägung, dass diese Situation durch den Mangel an gerichtlichen und behördlichen Rechtsbehelfen für EU-Bürger unter US-Recht weiter verschärft wird, insbesondere hinsichtlich der Überwachung für nachrichtendienstliche Zwecke;

Übermittlung an Drittländer mit der Angemessenheitsfeststellung

AQ. in der Erwägung, dass gemäß den enthüllten Informationen und den Ergebnissen der Überprüfung durch den LIBE-Ausschuss die nationalen Sicherheitsdienste Neuseelands, Kanadas und Australiens in großem Ausmaß an der Massenüberwachung elektronischer Kommunikation beteiligt waren und mit den USA im Rahmen des sogenannten „Fünf Augen“-Programms eng zusammengearbeitet und unter Umständen personenbezogene Daten von EU-Bürgern, die von der EU übermittelt wurden, untereinander ausgetauscht haben;

AR. in der Erwägung, dass die Schutzniveaus, die seitens des neuseeländischen „Privacy Act“ bzw. des „Protection and Electronic Documents Act“ Kanadas sichergestellt werden, in den Entscheidungen der Kommission 2013/65[1] und 2/2002 vom 20. Dezember 2001[2] für angemessen befunden wurden; in der Erwägung, dass die vorstehend genannten Enthüllungen zudem das Vertrauen in die Rechtssysteme dieser Länder hinsichtlich des Fortbestehens des den EU-Bürgern gewährten Schutzes ernsthaft erschüttern; in der Erwägung, dass dieser Gesichtspunkt von der Kommission nicht untersucht worden ist;

Übermittlungen auf der Grundlage von Vertragsklauseln und anderen Übereinkünften

AS. in der Erwägung, dass in der Richtlinie 95/46/EG festgelegt wird, dass die

[1] ABl. L 28 vom 30.1.2013, S. 12.
[2] ABl. L 2 vom 4.1.2002, S. 13.

internationale Datenübermittlung an ein Drittland auch mittels spezifischer Instrumente zulässig ist, wobei der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet;

AT. in der Erwägung, dass diese Garantien sich insbesondere aus entsprechenden Vertragsklauseln ergeben können;

AU. in der Erwägung, dass die Kommission gemäß Richtlinie 95/46/EG befugt ist, zu entscheiden, dass bestimmte Standardvertragsklauseln ausreichende Garantien gemäß dieser Richtlinie bieten, und in der Erwägung, dass die Kommission auf dieser Grundlage drei Standardvertragsklauseln für die Datenübermittlung an Verantwortliche und Datenverarbeiter (und Unterauftragsverarbeiter) in Drittländern verabschiedet hat;

AV. in der Erwägung, dass in den Beschlüssen der Kommission zur Einrichtung von Standardvertragsklauseln vorgesehen ist, dass die zuständigen Behörden in den Mitgliedstaaten ihre bestehenden Befugnisse ausüben können, um die Datenübermittlung aussetzen, wenn feststeht, dass der Datenimporteur oder der Unterauftragsverarbeiter nach den für ihn geltenden Rechtsvorschriften Anforderungen unterliegt, die ihn zwingen, vom anwendbaren Datenschutzrecht in einem Maß abzuweichen, das über die Beschränkungen hinausgeht, die im Sinne von Artikel 13 der Richtlinie 95/46/EG für eine demokratische Gesellschaft erforderlich sind, und dass sich diese Anforderungen wahrscheinlich sehr nachteilig auf die Garantien auswirken würden, die das anwendbare Datenschutzrecht und die Standardvertragsklauseln bieten, oder wenn eine hohe Wahrscheinlichkeit besteht, dass die im Anhang enthaltenen Standardvertragsklauseln derzeit oder künftig nicht eingehalten werden und die fortgesetzte Datenübermittlung für die betroffenen Personen das unmittelbare Risiko eines schweren Schadens bergen würde;

AW. in der Erwägung, dass nationale Datenschutzbehörden verbindliche unternehmensinterne Vorschriften (Binding Corporate Rules - BCR) ausgearbeitet haben, um die internationale Datenübermittlung innerhalb eines multinationalen Konzerns mit angemessenen Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte zu erleichtern; in der Erwägung, dass BCR vor ihrer Anwendung von den zuständigen Behörden der Mitgliedstaaten genehmigt werden müssen, nachdem letztere die Einhaltung des Datenschutzrechts der Union beurteilt haben; in der Erwägung, dass BCR für Auftragsverarbeiter in dem Bericht des LIBE-Ausschusses über die Datenschutzgrundverordnung abgelehnt werden, da sie dem für die Verarbeitung Verantwortlichen und der betroffenen Person keinerlei Kontrolle über die Gerichtsbarkeit einräumen würden, in der ihre Daten verarbeitet werden;

AX. in der Erwägung, dass das Europäische Parlament angesichts seiner Zuständigkeiten gemäß Artikel 218 AEUV dafür verantwortlich ist, den Wert der internationalen Vereinbarungen, denen es seine Zustimmung erteilt hat, fortlaufend zu überwachen;

Übermittlung auf Grundlage der TFTP- und PNR-Abkommen

AY. in der Erwägung, dass das Europäische Parlament in seiner Entschließung vom 23. Oktober 2013 seiner Besorgnis über die bekannt gewordenen Dokumente über die Tätigkeiten der NSA im Hinblick auf den direkten Zugang zu Zahlungsverkehrsdaten und damit verbundenen Daten, was einen klaren Verstoß gegen das TFTP-Abkommen und insbesondere dessen Artikel 1 darstellen würde, Ausdruck verliehen hat;

AZ. in der Erwägung, dass das Aufspüren von Terrorismusfinanzierung ein wichtiges Instrument bei der Bekämpfung der Finanzierung von Terrorismus und schwerer Straftaten ist, welches es den im Bereich der Terrorismusbekämpfung tätigen Ermittlern erlaubt, Verbindungen zwischen Ermittlungszielobjekten und anderen potenziell Verdächtigen aufzudecken, die mit größeren Terrornetzwerken, die der Terrorismusfinanzierung verdächtigt werden, in Verbindung stehen;

BA. in der Erwägung, dass das Parlament die Kommission ersucht hat, das Abkommen auszusetzen, und gefordert hat, dass alle einschlägigen Informationen und Dokumente unverzüglich für die Beratungen des Parlaments zur Verfügung gestellt werden; in der Erwägung, dass die Kommission weder dem Ersuchen noch der Forderung nachgekommen ist;

BB. in der Erwägung, dass die Kommission nach von den Medien veröffentlichten Behauptungen die Aufnahme von Konsultationen mit den USA gemäß Artikel 19 des TFTP-Abkommens beschlossen hat;in der Erwägung, dass Kommissarin Malmström den LIBE-Ausschuss am 27. November 2013 darüber informiert hat, dass die Kommission nach Zusammenkünften mit US-Behörden und angesichts der von den US-Behörden in Briefen und während der Treffen gegebenen Antworten beschlossen habe, die Konsultationen nicht weiterzuverfolgen, da es keine Hinweise darauf gebe, dass die US-Regierung in Widerspruch zu den Bestimmungen des Abkommens gehandelt habe, und da die Vereinigten Staaten schriftlich erklärt hätten, dass es keine direkte Sammlung von Daten im Widerspruch zu den Bestimmungen des TFTP-Abkommens gegeben habe; in der Erwägung, dass unklar ist, ob das Abkommen durch die US-Behörden umgangen wurde, indem sie solche Daten auf andere Weise erlangt haben, wie aus dem Schreiben der US-Behörden vom 18. September 2013[1] hervorgeht;

BC. in der Erwägung, dass die LIBE-Delegation während ihrer Reise nach Washington vom 28. bis 31. Oktober 2013 mit dem US-Finanzministerium zusammengetroffen ist; in der Erwägung, dass das US-Finanzministerium angab, seit Inkrafttreten des TFTP-Abkommens keinen Zugang zu SWIFT-Daten in der EU außerhalb des Rahmens des TFTP-Abkommens gehabt zu haben; in der Erwägung, dass sich das US-Finanzministerium weigerte, sich dazu zu äußern, ob andere US-Regierungsbehörden oder Ministerien außerhalb des Rahmens des TFTP-Abkommens auf SWIFT-Daten zugegriffen hätten oder ob die US-Regierung über die Massenüberwachung durch die NSA informiert gewesen sei; in der Erwägung, dass Glenn Greenwald am 18. Dezember 2013 bei der dem LIBE-Ausschuss durchgeführten Untersuchung

[1] In dem Schreiben heißt es, die US-Regierung bemühe sich um und erhalte Finanzinformationen, die von Regulierungs- und Strafverfolgungsbehörden, über diplomatische und nachrichtendienstliche Kanäle sowie durch den Austausch mit ausländischen Partnern erhoben werden. Das TFTP werde von der US-Regierung zur Erhebung von SWIFT-Daten genutzt, die nicht über andere Quellen bezogen werden.

angab, dass die NSA und dies GCHQ SWIFT-Netze anvisiert hätten;

BD. in der Erwägung, dass die Datenschutzbehörden Belgiens und der Niederlande am 13. November 2013 beschlossen, eine gemeinsame Untersuchung der Sicherheit von SWIFT-Zahlungen vorzunehmen, um zu ermitteln, ob Dritte unbefugten oder unrechtmäßigen Zugriff auf die Bankdaten europäischer Bürgerinnen und Bürger erhalten konnten[1];

BE. in der Erwägung, dass laut der gemeinsamen Überprüfung des PNR-Abkommens zwischen der EU und den USA auf Einzelfallbasis zur Unterstützung der Terrorismusbekämpfung und im Einklang mit den spezifischen Bestimmungen des Abkommens 23 Offenlegungen von PNR-Daten durch das amerikanische Ministerium für Heimatschutz (DHS) an die NSA erfolgten;

BF. in der Erwägung, dass in der gemeinsamen Überprüfung nicht erwähnt wird, dass bei der Verarbeitung personenbezogener Daten für nachrichtendienstliche Zwecke Nicht-US-Bürger unter der US-Gesetzgebung über keinen gerichtlichen oder behördlichen Rechtsbehelf zum Schutz ihrer Rechte verfügen und dass verfassungsmäßige Schutzvorkehrungen nur US-Bürgern gewährt werden; in der Erwägung, dass die in dem bestehenden PNR-Abkommen festgelegten Schutzvorkehrungen für EU-Bürger durch dieses Fehlen gerichtlicher oder behördlicher Rechte aufgehoben werden;

Übermittlung auf Grundlage des Abkommens zwischen der EU und den USA über Rechtshilfe in Strafsachen

BG. in der Erwägung, dass das Abkommen zwischen der EU und den USA über Rechtshilfe in Strafsachen vom 6. Juni 2003[2] am 1. Februar 2010 in Kraft trat und die Zusammenarbeit zwischen der EU und den USA zur wirksameren Bekämpfung von Kriminalität unter gebührender Berücksichtigung der Rechte von Einzelpersonen und der Rechtsstaatlichkeit vereinfachen soll;

Rahmenabkommen zum Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit („Rahmenabkommen")

BH. in der Erwägung, dass der Zweck dieses allgemeinen Abkommens die Einrichtung eines Rechtsrahmens für jede Übermittlung personenbezogener Daten zwischen der EU und den USA allein zum Zweck der Verhinderung, Ermittlung, Aufdeckung und Verfolgung von Straftaten einschließlich des Terrorismus im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen ist; in der Erwägung, dass Verhandlungen am 2. Dezember 2010 durch den Rat genehmigt wurden; in der Erwägung, dass dieses Abkommen von größter Wichtigkeit ist und als Grundlage für eine Erleichterung der Datenübermittlung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen dienen würde;

BI. in der Erwägung, dass mit diesem Abkommen klare und eindeutige rechtsverbindliche

[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] ABl. L 181 vom 19.7.2003, S. 25.

Grundsätze für die Datenverarbeitung festgelegt werden sollen und insbesondere das Recht der EU-Bürger auf gerichtlichen Zugang zu ihren personenbezogenen Daten in den USA und deren Korrektur und Löschung sowie das Recht auf effiziente behördliche und gerichtliche Rechtsbehelfe für EU-Bürger in den Vereinigten Staaten und unabhängige Aufsicht der Datenverarbeitung anerkannt werden sollen;

BJ. in der Erwägung, dass die Kommission in ihrer Mitteilung vom 27. November 2013 vorbrachte, dass das „Rahmenabkommen" zu einem hohen Schutzniveau für die Bürgerinnen und Bürger auf beiden Seiten des Atlantiks führen und das Vertrauen der Europäer in den Austausch von Daten zwischen der EU und den USA stärken und damit eine Grundlage für den weiteren Ausbau der Zusammenarbeit im Bereich der Sicherheit und der Partnerschaft zwischen der EU und den USA bieten sollte;

BK. in der Erwägung, dass Verhandlungen zu dem Abkommen nicht weit fortgeschritten sind, da sich die US-Regierung standhaft weigert, die wirksamen Rechte auf behördliche und gerichtliche Rechtsbehelfe für EU-Bürger anzuerkennen, und beabsichtigt, umfassende Ausnahmeregelungen zu den in diesem Abkommen enthaltenen Datenschutzgrundsätzen wie Zweckbindung, Vorratsdatenspeicherung oder die inländische oder ausländische Weitergabe von Daten vorzusehen;

Datenschutzreform

BL. in der Erwägung, dass der Rechtsrahmen der EU für den Datenschutz gegenwärtig mit dem Ziel überprüft wird, ein umfassendes, einheitliches, modernes und robustes System für alle Datenverarbeitungstätigkeiten in der Union einzurichten; in der Erwägung, dass die Kommission im Januar 2012 ein Paket von Legislativvorschlägen vorstellte, bestehend aus einer Datenschutzgrundverordnung, die die Richtlinie 95/46/EG[1] ersetzen und eine für die gesamte EU einheitliche Rechtsordnung schaffen wird, und einer Richtlinie[2], die einen harmonisierten Rechtsrahmen für alle von Strafverfolgungsbehörden zu Strafverfolgungszwecken durchgeführten Datenverarbeitungstätigkeiten festlegen und zum Abbau der derzeit bestehenden Unterschiede zwischen den nationalen Regelungen beitragen wird;

BM. in der Erwägung, dass der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) am 21. Oktober 2013 seine Legislativberichte zu den beiden Vorschlägen angenommen und beschlossen hat, Verhandlungen mit dem Rat aufzunehmen, damit die Rechtsakte noch in dieser Wahlperiode verabschiedet werden;

BN. in der Erwägung, dass es dem Europäischen Rat – wenngleich er bei einer Tagung am 24./25. Oktober 2013 die rasche Annahme eines soliden allgemeinen EU-Rahmens für den Datenschutz forderte, um das Vertrauen der Bürger und Unternehmen in die digitale Wirtschaft zu stärken – nach zweijährigen Beratungen noch immer nicht gelungen ist, einen allgemeinen Ansatz in Bezug auf die Datenschutzgrundverordnung und die Richtlinie[3] zu finden;

---

[1] COM(2012) 0011 vom 25.1.2012.
[2] COM(2012)0010 vom 25.1.2012.
[3] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/de/ec/139223.pdf.

IT-Sicherheit und Cloud-Computing

BO. in der Erwägung, dass das Cloud-Computing-Geschäft laut der Entschließung des Parlaments vom 10. Dezember[1] über ein bedeutendes Wachstums- und Beschäftigungspotenzial verfügt; in der Erwägung, dass der gesamte wirtschaftliche Wert des Cloud-Markts bis 2016 einen jährlichen Wert von 207 Mrd. US-Dollar erreicht haben wird, was einer Verdopplung des Wertes von 2012 entspricht;

BP. in der Erwägung, dass das Niveau des Datenschutzes in einer Cloud-Computing-Umgebung grundsätzlich nicht niedriger sein darf als in jedem anderen Datenverarbeitungsprozess; in der Erwägung, dass das Datenschutzrecht der Union aufgrund seiner technologischen Neutralität bei Cloud-Computing-Diensten innerhalb der EU schon heute uneingeschränkt Anwendung findet;

BQ. in der Erwägung, dass Geheimdienste durch Massenüberwachungsmaßnahmen Zugriff auf personenbezogene Daten erhalten, die von EU-Bürgern im Rahmen von Vereinbarungen über Cloud-Dienste bei großen US-amerikanischen Cloud-Anbietern gespeichert oder anderweitig verarbeitet werden; in der Erwägung, dass die US-amerikanischen Geheimdienste auf personenbezogene Daten zugegriffen haben, die auf in der EU befindlichen Servern gespeichert sind oder anderweitig verarbeitet werden, indem sie die internen Netze von Yahoo und Google anzapften; in der Erwägung, dass derartige Aktivitäten eine Verletzung der internationalen Verpflichtungen und der europäischen Grundrechtsnormen, einschließlich des Rechts auf die Achtung des Privat- und Familienlebens, auf die Vertraulichkeit der Kommunikation, auf Unschuldsvermutung, auf die Freiheit der Meinungsäußerung, auf Informationsfreiheit, auf Versammlungs- und Vereinigungsfreiheit und auf unternehmerische Freiheit darstellen; in der Erwägung, dass nicht ausgeschlossen ist, dass auch in den Cloud-Diensten von öffentlichen Behörden, Unternehmen und Einrichtungen der Mitgliedstaaten gespeicherte Daten von den Geheimdiensten abgegriffen wurden;

BR. in der Erwägung, dass die US-Geheimdienste eine Strategie verfolgen, mit der sie kryptografische Protokolle und Produkte systematisch unterlaufen, um selbst verschlüsselte Kommunikation abhören zu können; in der Erwägung, dass die National Security Agency der Vereinigten Staaten zu einer Vielzahl sogenannter „Zero-Day-Exploits“ – Schwachstellen in der IT-Sicherheit, die der Öffentlichkeit oder dem Produktanbieter noch unbekannt sind – Informationen gesammelt hat; in der Erwägung, dass derartige Aktivitäten die weltweiten Bemühungen zur Verbesserung der IT-Sicherheit massiv untergraben;

BS. in der Erwägung, dass die Tatsache, dass die Geheimdienste auf die personenbezogenen Daten der Nutzer von Online-Diensten zugegriffen haben, das Vertrauen der Bürgerinnen und Bürger in solche Dienste schwer beschädigt hat und sich daher nachteilig auf Unternehmen auswirkt, die in die Entwicklung von neuen Diensten, die große Datenmengen („Big Data“) nutzen, und in neue Anwendungen wie dem „Internet der Dinge“ investieren;

[1] A7-0353/2013 - PE506.114v2.00.

BT. in der Erwägung, dass IT-Anbieter häufig Produkte anbieten, deren IT-Sicherheit nicht ordnungsgemäß geprüft wurde oder bei denen der Anbieter in einigen Fällen sogar gezielt Backdoors eingebaut hat; in der Erwägung, dass der Mangel an Haftungsregelungen für Software-Anbieter eine Situation herbeigeführt hat, die im Gegenzug von Geheimdiensten ausgenutzt wird, aber auch die Gefahr von Angriffen von anderer Seite birgt;

BU. in der Erwägung, dass es für Unternehmen, die neue Dienste und Anwendungen dieser Art anbieten, von grundlegender Bedeutung ist, die Datenschutzbestimmungen einzuhalten und die Privatsphäre der Personen, deren Daten erfasst, verarbeitet und ausgewertet werden, zu wahren, damit bei den Bürgerinnen und Bürgern ein hohes Maß an Vertrauen erhalten bleibt;

Demokratische Aufsicht über Nachrichtendienste

BV. in der Erwägung, dass den Geheimdiensten in demokratischen Gesellschaften besondere Befugnisse und Kompetenzen verliehen wurden, um die Grundrechte, die Demokratie und Rechtsstaatlichkeit, die Bürgerrechte und den Staat gegen innere und äußere ernsthafte Bedrohungen zu schützen, und dass sie der demokratischen Rechenschaftspflicht und gerichtlicher Kontrolle unterliegen; in der Erwägung, dass ihnen ausschließlich zu diesem Zweck besondere Befugnisse und Kompetenzen verliehen wurden; in der Erwägung, dass sie von diesen Befugnissen im Rahmen der gesetzlichen Beschränkungen nach Maßgabe der Grundrechte, der Demokratie und der Rechtsstaatlichkeit Gebrauch machen müssen und dass deren Ausübung sorgfältig geprüft werden muss, da sie sonst an Legitimität verlieren und Gefahr laufen, die Demokratie zu untergraben;

BW. in der Erwägung, dass den Nachrichtendiensten ein gewisser Grad der Geheimhaltung zugestanden wird – um laufende Operationen nicht zu gefährden, Arbeitsweisen nicht preiszugeben oder das Leben von Agenten nicht in Gefahr zu bringen –, die Geheimhaltung jedoch nicht die Bestimmungen über die demokratische und gerichtliche Kontrolle und Untersuchung nachrichtendienstlicher Tätigkeiten sowie über die Transparenz, besonders mit Blick auf die Wahrung der Grundrechte, der Demokratie und der Rechtsstaatlichkeit, die allesamt Eckpfeiler in einer demokratischen Gesellschaft sind, außer Kraft setzen darf;

BX. in der Erwägung, dass die meisten der bestehenden nationalen Kontrollmechanismen und -gremien in den 1990er-Jahren geschaffen oder neu organisiert und nicht unbedingt an die raschen politischen und technischen Fortschritte des letzten Jahrzehnts angepasst wurden, die zu einer zunehmenden internationalen Zusammenarbeit im nachrichtendienstlichen Bereich, auch durch den umfangreichen Austausch personenbezogener Daten, geführt und die Grenze zwischen nachrichtendienstlichen und polizeilichen Tätigkeiten häufig verwischt haben;

BY. in der Erwägung, dass die demokratische Kontrolle der nachrichtendienstlichen Tätigkeiten trotz des zunehmenden Informationsaustauschs unter den EU-Mitgliedstaaten und zwischen den Mitgliedstaaten und Drittländern noch immer ausschließlich auf nationaler Ebene stattfindet; in der Erwägung, dass eine zunehmende Diskrepanz besteht zwischen dem Grad der internationalen

Zusammenarbeit einerseits und den auf die nationale Ebene beschränkten Kontrollkapazitäten andererseits, weshalb die demokratische Kontrolle unzureichend und unwirksam ist;

BZ. in der Erwägung, dass die nationalen Kontrollgremien häufig keinen ungehinderten Zugang zu den von ausländischen Nachrichtendiensten übermittelten Aufklärungsdaten haben und dass dies zu Lücken führen kann, die den internationalen Austausch von Informationen ohne angemessene Überprüfung zur Folge haben können; in der Erwägung, dass dieses Problem noch verschärft wird durch die sogenannte „Drittparteiregel“ oder den Grundsatz der „Kontrolle durch den Urheber“, mit dem Urheber in die Lage versetzt werden sollen, die Kontrolle über die Weiterverbreitung ihrer sensiblen Informationen zu behalten, der aber leider häufig so ausgelegt wird, dass er auch für die Kontrolle der Dienste aufseiten des Empfängers gilt;

CA. in der Erwägung, dass private und öffentliche Reformvorhaben zur Förderung der Transparenz von entscheidender Bedeutung für die Schaffung von öffentlichem Vertrauen in die Tätigkeiten der Nachrichtendienste sind; in der Erwägung, dass die Rechtssysteme Unternehmen nicht davon abhalten sollten, die Öffentlichkeit darüber zu informieren, wie sie mit allen Arten von Anfragen von staatlicher Seite und gerichtlichen Anordnungen zur Freigabe von Nutzerdaten umgehen, einschließlich der Möglichkeit, aggregierte Informationen zur Anzahl der Anfragen und Anordnungen, denen nachgekommen bzw. nicht nachgekommen wurde, offenzulegen;

Wichtigste Ergebnisse

1. ist der Ansicht, dass jüngste Enthüllungen durch Informanten und Journalisten in der Presse gemeinsam mit den im Rahmen dieser Untersuchung abgegebenen Sachverständigengutachten, Zugeständnissen von staatlichen Stellen und der Tatsache, dass auf diese Anschuldigungen nicht genügend reagiert wurde, einen zwingenden Beweis für die Existenz weit verzweigter, komplexer und hochmoderner Systeme darstellen, die von den Geheimdiensten der USA und einiger Mitgliedstaaten entwickelt wurden, um die Kommunikationsdaten, darunter Inhalts-, Standort- und Verbindungsdaten, aller Bürger weltweit in bisher ungekanntem Ausmaß, wahllos und ohne Vorliegen eines Verdachts zu sammeln, zu speichern und zu analysieren;

2. weist insbesondere auf die Programme des US-Geheimdienstes NSA hin, die die Massenüberwachung von EU-Bürgern ermöglichen, indem sie sich des direkten Zugriffs auf die zentralen Server der führenden US-amerikanischen Internetkonzerne (PRISM-Programm), der Analyse von Inhalten und Verbindungsdaten (Xkeyscore), der Umgehung von Verschlüsselung im Internet (BULLRUN-Programm), des Zugangs zu Computer- und Telefonnetzen und des Zugangs zu Standortdaten bedienen, sowie auf die Systeme des britischen Geheimdienstes GCHQ, wie etwa das Programm zur Überwachung der Kommunikation über transatlantische Glasfaserkabel (Tempora-Programm) und das Entschlüsselungsprogramm Edgehill, die gezielten Mittelsmannangriffe auf Informationssysteme (Programme „Quantumtheory“ und „Foxacid“) und das Abfangen und die Speicherung von täglich 200 Millionen SMS-Textnachrichten (Dishfire-Programm) zugreifen;

3. nimmt die Behauptungen zur Kenntnis, wonach der britische Geheimdienst GCHQ in die Systeme des Unternehmens Belgacom eingedrungen sein und diese angezapft haben soll; nimmt die Erklärungen von Belgacom zur Kenntnis, wonach das Unternehmen weder bestätigen noch dementieren könne, dass Organe der EU Ziel der Überwachungsmaßnahmen oder von ihnen betroffen waren, und wonach die verwendete Malware äußerst kompliziert gewesen sei und nicht ohne den Einsatz erheblicher finanzieller und personeller Mittel, die Privatleuten oder Hackern nicht zur Verfügung stünden, entwickelt und genutzt hätte werden können;

4. betont, dass das Vertrauen zwischen den beiden transatlantischen Partnern, das Vertrauen zwischen den Bürgern und ihren Regierungen, das Vertrauen in das Funktionieren der demokratischen Institutionen auf beiden Seiten des Atlantiks, das Vertrauen in die Achtung der Rechtstaatlichkeit sowie das Vertrauen in die Sicherheit von IT-Dienstleistungen und Kommunikation zutiefst erschüttert ist; ist der Meinung, dass es dringend eines sofortigen und umfassenden Abwehrplans mit einer Reihe von Maßnahmen, deren Umsetzung öffentlich nachgeprüft werden kann, bedarf, um das Vertrauen auf all diesen Ebenen wiederherzustellen;

5. nimmt zur Kenntnis, dass mehrere Regierungen behaupten, die Programme zur Massenüberwachung seien notwendig für die Terrorismusbekämpfung; verurteilt Terrorismus nachdrücklich, ist jedoch der festen Überzeugung, dass der Kampf gegen den Terrorismus an sich niemals als Rechtfertigung für ungezielte, geheime oder sogar rechtswidrige Programme zur Massenüberwachung dienen kann; sieht solche Programme als unvereinbar mit den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit in einer demokratischen Gesellschaft an;

6. verweist auf die feste Überzeugung der EU, dass ein angemessenes Gleichgewicht zwischen Sicherheitsmaßnahmen und dem Schutz der bürgerlichen Freiheiten und Grundrechte gefunden und gleichzeitig die größtmögliche Achtung der Privatsphäre und des Datenschutzes gewährleistet werden muss;

7. äußert starke Zweifel daran, dass eine Datenerhebung dieser Größenordnung nur vom Kampf gegen den Terrorismus geleitet ist, da bei ihr alle möglichen Daten von allen Bürgern gesammelt werden; weist daher darauf hin, dass möglicherweise andere Absichten, darunter politische Spionage oder Wirtschaftsspionage, eine Rolle spielen könnten, die umfassend ausgeräumt werden müssen;

8. stellt die Vereinbarkeit der von einigen Mitgliedstaaten in großem Stil durchgeführten Wirtschaftsspionagetätigkeiten mit dem in Titel I bzw. Titel VII des Vertrags über die Arbeitsweise der Europäischen Union verankerten EU-Binnenmarkt und dem Wettbewerbsrecht in Frage; bekräftigt den in Artikel 4 Absatz 3 des Vertrags über die Europäische Union verankerten Grundsatz der loyalen Zusammenarbeit sowie den Grundsatz, wonach die Mitgliedstaaten alle Maßnahmen unterlassen, die die Verwirklichung der Ziele der Union gefährden könnten;

9. stellt fest, dass die internationalen Verträge, die Rechtsvorschriften der EU und der USA und die nationalen Kontrollmechanismen nicht für das nötige Maß an Aufsicht und demokratischer Kontrolle gesorgt haben;

10. verurteilt die in gigantischem Ausmaß erfolgte systematische und pauschale Erfassung der personenbezogenen, oft auch intimen persönlichen Daten unschuldiger Menschen; betont, dass der Einsatz von Systemen für die willkürliche Massenüberwachung durch die Geheimdienste einen schwerwiegenden Eingriff in die Grundrechte der Bürger darstellt; hebt hervor, dass das Recht auf Achtung der Privatsphäre kein Luxus ist, sondern einen Grundpfeiler der freien und demokratischen Gesellschaft darstellt; weist zudem auf die möglicherweise gravierenden Auswirkungen der Massenüberwachung auf die Pressefreiheit, die Gedankenfreiheit, das Recht auf freie Meinungsäußerung und auf die Versammlungs- und Vereinigungsfreiheit hin sowie darauf, dass sie ein erhebliches Potenzial für den Missbrauch von Informationen birgt, da die gesammelten Daten gegen politische Feinde eingesetzt werden könnten; betont, dass die beschriebenen Massenüberwachungsmaßnahmen auch illegale Handlungen seitens der Geheimdienste einschließen und Fragen bezüglich der extraterritorialen Wirkung nationaler Gesetze aufwerfen;

11. hält es für äußerst wichtig, dass das Berufsgeheimnis für Anwälte, Journalisten, Ärzte und andere reglementierte Berufe vor Massenüberwachung geschützt wird; weist darauf hin, dass jegliche Unsicherheit über die Vertraulichkeit der Kommunikation zwischen Anwälten und ihren Mandanten sich negativ auf das Recht der Bürger auf Zugang zu anwaltlicher Beratung und zum Justizwesen und auf das Recht auf ein faires Verfahren auswirken könnte;

12. erachtet die Überwachungsprogramme als weiteren Schritt hin zur Einrichtung eines echten Präventionsstaats, in dem ein Paradigmenwechsel des in demokratischen Gesellschaften etablierten Strafrechts erfolgt, demzufolge jeder Eingriff in die Grundrechte eines Verdächtigen von einem Richter oder Staatsanwalt auf der Grundlage eines begründeten Verdachts genehmigt und gesetzlich geregelt werden muss, und stattdessen eine Mischung aus Strafverfolgungs- und Geheimdienstaktivitäten propagiert wird, die unklaren und verwässerten rechtlichen Bestimmungen unterliegen und oftmals nicht mit den demokratischen Kontrollmechanismen und den Grundrechten, insbesondere der Unschuldsvermutung, vereinbar sind; verweist in diesem Zusammenhang auf die Entscheidung des Bundesverfassungsgerichts[1], nach der eine präventive Rasterfahndung nur dann zulässig ist, wenn nachweislich eine konkrete Gefahr für andere hochrangige Rechtsgüter vorliegt, weshalb eine allgemeine Bedrohungslage oder außenpolitische Spannungslagen nicht ausreichen, um derartige Maßnahmen zu rechtfertigen;

13. ist davon überzeugt, dass geheime Gesetze und Gerichte eine Verletzung der Rechtsstaatlichkeit darstellen; weist darauf hin, dass die Urteile von Gerichten und die Entscheidungen von Verwaltungsbehörden in Nicht-EU-Staaten, die die Übermittlung personenbezogener Daten direkt oder indirekt genehmigen, in keiner Weise anerkannt oder vollstreckt werden dürfen, es sei denn, es gibt ein Abkommen über Amtshilfe oder ein zwischen dem ersuchenden Drittstaat und der Union oder einem Mitgliedstaat geltendes internationales Übereinkommen und eine vorherige Genehmigung durch die zuständige Aufsichtsbehörde; erinnert daran, dass Urteile von Geheimgerichten und Entscheidungen von Verwaltungsbehörden eines Nicht-EU-Landes, das

[1] 1 BvR 518/02 vom 4.April.2006.

Überwachungsaktivitäten insgeheim direkt oder indirekt genehmigt, nicht anerkannt oder vollstreckt werden dürfen;

14. weist darauf hin, dass die genannten Befürchtungen durch die rasche technische und gesellschaftliche Entwicklung noch verstärkt werden, da das Internet und mobile Geräte aus dem modernen Alltag nicht mehr wegzudenken sind („allgegenwärtige Datenverarbeitung“) und das Geschäftsmodell der meisten Internetanbieter auf der Verarbeitung personenbezogener Daten basiert; vertritt die Auffassung, dass es sich um ein Problem bisher ungekannten Ausmaßes handelt; stellt fest, dass dies zu einer Situation führen kann, in der die Infrastruktur für die massenhafte Erhebung und Verarbeitung von Daten im Falle eines politischen Führungswechsels missbraucht werden kann;

15. stellt fest, dass weder die öffentlichen Institutionen noch die Bürger der EU sicher sein können, dass ihre IT-Systeme und ihre Privatsphäre vor Angriffen durch gut ausgerüstete Eindringlinge geschützt sind („keine 100%-ige IT-Sicherheit“); stellt fest, dass es für maximale IT-Sicherheit erforderlich ist, dass man in Europa bereit ist, ausreichende personelle und finanzielle Mittel für die Aufrechterhaltung der Unabhängigkeit und Eigenständigkeit auf dem Gebiet der IT bereitzustellen;

16. weist die Auffassung, dass alle Fragen in Verbindung mit Programmen zur Massenüberwachung lediglich die nationale Sicherheit betreffen und daher ausschließlich der Zuständigkeit der Mitgliedstaaten unterliegen, mit Nachdruck zurück; wiederholt, dass die Mitgliedstaaten sich in ihrem Handeln zum Schutz der nationalen Sicherheit uneingeschränkt an die Vorgaben des EU-Rechts und der EMRK zu halten haben; verweist auf ein kürzlich ergangenes Urteil des Gerichtshofs, wonach „es zwar Sache der Mitgliedstaaten [ist], die geeigneten Maßnahmen zur Gewährleistung ihrer inneren und äußeren Sicherheit zu ergreifen, [...] der Umstand, dass eine Entscheidung die Sicherheit des Staates betrifft, für sich allein genommen [jedoch] nicht zur Unanwendbarkeit des Rechts der Union führen [kann]“[1]; erinnert ferner daran, dass es um den Schutz der Privatsphäre aller EU-Bürger geht und dass die Sicherheit und Zuverlässigkeit aller Kommunikationsnetze der EU in Gefahr sind; ist daher der Meinung, dass Diskussionen und Maßnahmen auf EU-Ebene nicht nur legitim, sondern auch notwendig für den Erhalt der Autonomie der EU sind;

17. begrüßt die Diskussionen, die derzeit in verschiedenen Teilen der Welt um den Gegenstand dieser Untersuchung geführt werden, sowie die diesbezüglichen Untersuchungen und Überprüfungen, auch durch die Unterstützung der Zivilgesellschaft; weist auf den von den weltweit führenden Technologieunternehmen unterzeichneten Aufruf zu einer „Global Government Surveillance Reform“ (Globale Reform der staatlichen Überwachung) hin, in dem die Unternehmen grundlegende Veränderungen in den einzelstaatlichen Überwachungsgesetzen – darunter ein internationales Verbot der Sammelerhebung von Daten – fordern, damit das Vertrauen der Öffentlichkeit in das Internet und in ihre Unternehmen erhalten bleibt; weist auf den Aufruf von hunderten führenden Akademikern[2], Organisationen der

[1] Urteil in der Rechtssache C-300/11, ZZ/Secretary of State for the Home Department vom 4. Juni.2013.
[2] www.academicsagainstsurveillance.net.

Zivilgesellschaft[1] und 562 internationalen Autoren, darunter fünf Nobelpreisträger, zur Beendigung der Massenüberwachung hin; nimmt die kürzlich veröffentlichten Empfehlungen der vom US-Präsidenten eingesetzten „Review Group on Intelligence and Communications Technologies“ und den Bericht des „Privacy and Civil Liberties Oversight Board“ über das Programm zur Aufzeichnung von Telefongesprächen, das gemäß Abschnitt 15 des USA-PATRIOT Act durchgeführt wurde, sowie über die Tätigkeiten des für die Überwachung ausländischer Geheimdienste zuständigen Gerichts[2] mit großem Interesse zur Kenntnis; fordert die Regierungen nachdrücklich auf, diese Aufrufe und Empfehlungen in vollem Umfang zu berücksichtigen und ihre nationalen Rahmenbedingungen für die Arbeit ihrer Geheimdienste so zu überarbeiten, dass sie angemessene Schutzmaßnahmen und Kontrollmechanismen vorsehen;

18. spricht den Institutionen und Experten, die zu dieser Untersuchung beigetragen haben, seine Anerkennung aus; bedauert, dass die Behörden mehrerer Mitgliedstaaten eine Zusammenarbeit im Rahmen der vom Europäischen Parlament im Interesse der Bürger durchgeführten Untersuchung abgelehnt haben; begrüßt die Offenheit mehrerer Kongressmitglieder und Abgeordneter nationaler Parlamente;

19. ist sich dessen bewusst, dass innerhalb so kurzer Zeit lediglich eine vorläufige Untersuchung aller seit Juli 2013 aufgetauchten Fragen durchgeführt werden konnte; erkennt sowohl das Ausmaß der Enthüllungen als auch die Tatsache an, dass deren Ende noch nicht abzusehen ist; verfolgt daher einen vorausschauenden Ansatz bestehend aus einigen konkreten Vorschlägen und einem Mechanismus für Folgemaßnahmen in der nächsten Wahlperiode, die sicherstellen sollen, dass die Erkenntnisse ganz oben auf der politischen Agenda der EU bleiben;

20. beabsichtigt, von der neuen Kommission, die nach den Wahlen im Mai 2014 ernannt werden wird, ehrgeizige politische Zusagen zu verlangen, dass sie die Vorschläge und Empfehlungen dieser Untersuchung umsetzen wird; erwartet von den Kandidaten, dass sie in den bevorstehenden Anhörungen der neuen Kommissionsmitglieder im Europäischen Parlament ein angemessenes Engagement erkennen lassen;

Empfehlungen

21. fordert die US-Behörden und die EU-Mitgliedstaaten, in denen das noch nicht geschehen ist, auf, die pauschale Massenüberwachung zu verbieten;

22. fordert alle EU-Mitgliedstaaten, darunter insbesondere die Teilnehmer an den sogenannten „9-Eyes“- und „14-Eyes“ Programmen[3], auf, ihre nationalen Rechtsvorschriften und Verfahren im Bereich geheimdienstlicher Tätigkeiten – einschließlich (strategischer) Überwachungsbefugnisse, Genehmigungsverfahren und Überwachungsmechanismen – umfassend zu prüfen und gegebenenfalls zu

[1] www.stopspyingonus.com and www.en.necessaryandproportionate.org.
[2] http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf.
[3] Das “9-Eyes”-Programm umfasst die USA, das VK, Kanada, Australien, Neuseeland, Dänemark, Frankreich, Norwegen und die Niederlande; das “14-Eyes”-Programm umfasst diese Länder und zusätzlich Deutschland, Belgien, Italien, Spanien und Schweden.

überarbeiten, um sicherzustellen, dass diese der parlamentarischen und gerichtlichen Kontrolle und der Kontrolle der Öffentlichkeit unterworfen sind, dass sie die Grundsätze Gesetzesmäßigkeit, Notwendigkeit, Verhältnismäßigkeit, rechtsstaatliches Verfahren, Benachrichtigung des Nutzers und Transparenz, wie auch in der Aufstellung bewährter Verfahren der UN und in den Empfehlungen der Venedig-Kommission ausgeführt wird, befolgen und dass sie mit den Normen der Europäischen Menschenrechtskonvention sowie mit den Menschenrechtsverpflichtungen der Mitgliedstaaten, insbesondere hinsichtlich Datenschutz, Privatsphäre und Unschuldsvermutung, in Einklang stehen;

23. fordert alle EU-Mitgliedstaaten und unter Hinweis auf seine Entschließung vom 4. Juli 2013 und die Anhörungen vor dem Untersuchungsausschuss insbesondere das Vereinigte Königreich, Frankreich, Deutschland, Schweden, die Niederlande und Polen auf, dafür Sorge zu tragen, dass ihre aktuellen oder künftigen nationalen Rechtsrahmen und Kontrollmechanismen im Bereich geheimdienstlicher Tätigkeiten mit den Normen der Europäischen Menschenrechtskonvention und den Datenschutzgesetzen der Europäischen Union in Einklang stehen; fordert diese Mitgliedstaaten auf, die Anschuldigungen von Massenüberwachung, einschließlich der Massenüberwachung grenzüberschreitender Telekommunikation, von ungezielter Überwachung bei der kabelgebundenen Kommunikation, möglicher Vereinbarungen zwischen Nachrichtendiensten und Telekommunikationsunternehmen über den Zugang zu und den Austausch von personenbezogenen Daten sowie den Zugang zu transatlantischen Kabeln, von US-Geheimdienstmitarbeitern und -Ausrüstung auf dem Hoheitsgebiet der EU ohne Kontrolle von Überwachungsmaßnahmen, und ihre Vereinbarkeit mit EU-Recht zu klären; fordert die nationalen Parlamente dieser Länder auf, die Zusammenarbeit ihrer Geheimdienstaufsichtsgremien auf europäischer Ebene zu intensivieren;

24. fordert insbesondere das Vereinigte Königreich angesichts der ausführlichen Medienberichte über Massenüberwachung durch den Geheimdienst GCHQ auf, seinen derzeitigen Rechtsrahmen, der durch das komplexe Zusammenspiel dreier eigenständiger Gesetze – des Human Rights Act 1998, des Intelligence Services Act 1994 und des Regulation of Investigatory Powers Act 2000 – gegeben ist, zu überarbeiten;

25. nimmt die Überarbeitung des niederländischen Gesetzes über Nachrichten- und Sicherheitsdienste von 2002 zur Kenntnis (Bericht der Dessens-Kommission vom 2. Dezember 2013); unterstützt die Empfehlungen der Überprüfungskommission, die auf eine Verbesserung der Transparenz, der Kontrolle und der Beaufsichtigung der niederländischen Nachrichtendienste abzielen; fordert die Niederlande auf, davon abzusehen, die Befugnisse der Nachrichtendienste dahingehend auszuweiten, dass die ungezielte und großflächige Überwachung auch bei der kabelgebundenen Kommunikation unschuldiger Bürgerinnen und Bürger erfolgen könnte, insbesondere angesichts der Tatsache, dass sich einer der größten Internetaustauschpunkte in Amsterdam befindet (AMS-IX); ruft zur Vorsicht bei der Festlegung des Mandats und der Fähigkeiten der neuen Joint SIGINT Cyber Unit sowie zur Vorsicht im Hinblick auf die Anwesenheit und Tätigkeit von Mitarbeitern der US-Nachrichtendienste auf niederländischem Hoheitsgebiet auf;

26. fordert die Mitgliedstaaten auf, auch dann, wenn sie durch ihre Nachrichtendienste vertreten werden, keine widerrechtlich gesammelten Daten von Drittstaaten anzunehmen und keine Überwachungsmaßnahmen auf ihrem Hoheitsgebiet durch Regierungen oder Behörden von Drittstaaten zuzulassen, die im Widerspruch zu nationalem Recht oder zu den in internationalen Übereinkünften oder Rechtsakten der EU verankerten rechtlichen Bestimmungen, darunter auch die Bestimmungen zum Schutz der Menschenrechte gemäß dem EUV, der EMRK und der EU-Grundrechtecharta, stehen;

27. fordert die Mitgliedstaaten auf, unverzüglich ihrer positiven Verpflichtung im Rahmen der Europäischen Menschenrechtskonvention nachzukommen, wonach sie ihre Bürger vor Überwachungsmaßnahmen durch Drittstaaten oder durch ihre eigenen Nachrichtendienste, die den Anforderungen der Konvention zuwiderlaufen, schützen sollten, auch wenn diese zum Schutz der nationalen Sicherheit durchgeführt werden, und sicherzustellen, dass der Rechtsstaat infolge der extraterritorialen Anwendung der Gesetze eines Drittlands nicht geschwächt wird;

28. fordert den Generalsekretär des Europarats auf, das Verfahren gemäß Artikel 52 einzuleiten, wonach „[jede Hohe Vertragspartei auf] Anfrage des Generalsekretärs des Europarats erläutert [...], auf welche Weise die wirksame Anwendung aller Bestimmungen dieser Konvention in ihrem innerstaatlichen Recht gewährleistet wird“;

29. fordert die Mitgliedstaaten auf, unverzüglich geeignete Maßnahmen, einschließlich gerichtlicher Schritte, gegen die Verletzung ihrer Souveränität und des allgemeinen Völkerrechts, die der Einsatz von Programmen zur Massenüberwachung darstellt, einzuleiten; fordert die Mitgliedstaaten zudem auf, alle verfügbaren internationalen Maßnahmen zu nutzen, um die Grundrechte der EU-Bürger zu verteidigen, insbesondere indem sie das zwischenstaatliche Beschwerdeverfahren gemäß Artikel 41 des Internationalen Pakts über bürgerliche und politische Rechte (IPBPR) auslösen;

30. fordert die USA auf, ihre Rechtsvorschriften unverzüglich zu überarbeiten, um sie mit dem Völkerrecht in Einklang zu bringen, das Recht auf Privatsphäre und andere Rechte der EU-Bürger anzuerkennen, Rechtsbehelfe für EU-Bürger bereitzustellen, EU-Bürgern die gleichen Rechte einzuräumen wie US-Bürgern und das Fakultativprotokoll des IPBPR zu unterzeichnen, das Beschwerden durch Einzelpersonen ermöglicht;

31. begrüßt in diesem Zusammenhang die von US-Präsident Barack Obama erlassene Grundsatzrichtlinie vom 17. Januar 2014 und seine Äußerungen dazu als einen Schritt zur Einschränkung der Befugnisse bei Überwachungs- und Datenverarbeitungstätigkeiten zu Zwecken der nationalen Sicherheit sowie zu einer Gleichbehandlung der personenbezogenen Informationen aller Einzelpersonen ungeachtet ihrer Staatsangehörigkeit oder ihres Wohnsitzes durch die US-Geheimdienste; erwartet jedoch mit Blick auf die Beziehungen zwischen der EU und den Vereinigten Staaten weitere konkrete Schritte, die in erster Linie darauf abzielen, das Vertrauen in transatlantische Datenübermittlungen zu stärken und verbindliche

Garantien für durchsetzbare Rechte zum Schutz der Privatsphäre von EU-Bürgern zu schaffen, wie in diesem Bericht ausführlich dargelegt;

32. unterstreicht seine ernsthaften Bedenken hinsichtlich der vom Ausschuss für das Übereinkommen über Computerkriminalität des Europarats verfolgten Auslegung von Artikel 32 des Übereinkommens über Computerkriminalität vom 23. November 2001 (Budapester Übereinkommen), der den grenzüberschreitenden Zugriff auf gespeicherte Computerdaten im Falle der Zustimmung oder öffentlichen Zugänglichkeit regelt, und spricht sich gegen die Unterzeichnung eines Zusatzprotokolls oder von Leitlinien aus, mit denen der Anwendungsbereich dieser Bestimmung über die geltenden Regelungen im Rahmen dieses Übereinkommens hinaus noch ausgeweitet wird, da diese Regelungen bereits eine wesentliche Ausnahme vom Territorialitätsgrundsatz darstellen, indem sie zu einem ungehinderten Fernzugriff von Strafverfolgungsbehörden auf Server und Computersysteme in anderen Gerichtsbarkeiten führen könnten, ohne dass sich diese der Rechtshilfeabkommen und anderer Instrumente der justiziellen Zusammenarbeit bedienen, die zur Sicherung der Grundrechte der Einzelnen, einschließlich des Rechts auf Datenschutz und auf ein faires Verfahren, eingerichtet wurden, und insbesondere das Übereinkommen des Europarats Nr. 108;

33. fordert die Kommission auf, vor Juli 2014 zu bewerten, inwieweit die Verordnung (EG) Nr. 2271/96 auf Gesetzeskollisionen bei der Übermittlung personenbezogener Daten anwendbar ist;

34. fordert die Grundrechte-Agentur auf, genauere Untersuchungen über den Schutz der Grundrechte im Zusammenhang mit der Überwachung und insbesondere der derzeitigen Rechtslage von EU-Bürgern im Hinblick auf Rechtsmittel, die ihnen bezüglich solcher Praktiken zur Verfügung stehen, durchzuführen;

Internationale Datenübermittlungen

US-Datenschutzrechtsrahmen und „Safe-Harbour"-Vereinbarung mit den USA

35. stellt fest, dass es sich bei den Unternehmen, die laut den Enthüllungen der Medien von der flächendeckenden Überwachung von Datensubjekten in der EU durch den US-Geheimdienst NSA betroffen waren, um Unternehmen handelt, die sich öffentlich zur Einhaltung der Grundsätze des „sicheren Hafens" („Safe Harbour") verpflichtet haben, und dass die „Safe-Harbour"-Vereinbarung das Rechtsinstrument ist, das für die Übermittlung personenbezogener Daten aus der EU in die USA verwendet wird (Beispiele sind Google, Microsoft, Yahoo!, Facebook, Apple und LinkedIn); erklärt sich besorgt, dass diese Unternehmen den Informations- und Kommunikationsfluss zwischen ihren Datenzentren nicht verschlüsselt haben, wodurch sie den Geheimdiensten das Abfangen von Informationen ermöglichen; begrüßt die diesbezüglichen Bemühungen einiger US-Unternehmen, die Vorhaben zur Verschlüsselung der Datenflüsse zwischen ihren globalen Datenzentren zu beschleunigen;

36. ist der Ansicht, dass der in großem Stil erfolgte Zugriff der US-Geheimdienste auf personenbezogene Daten der EU, die nach der „Safe-Harbour"-Vereinbarung

verarbeitet werden, nicht die Kriterien für eine Ausnahmeregelung aus Gründen der „nationalen Sicherheit“ erfüllt;

37. vertritt die Auffassung, dass die Grundsätze des „sicheren Hafens“ den EU-Bürgern unter den jetzigen Umständen keinen angemessenen Schutz bieten und dass diese Übermittlungen daher anderen Instrumenten wie etwa Vertragsbestimmungen oder verbindlichen unternehmensinternen Vorschriften unterliegen sollten, sofern diese Instrumente konkrete Sicherheits- und Schutzmaßnahmen vorsehen und nicht durch andere Rechtsinstrumente umgangen werden;

38. ist der Auffassung, dass es der Kommission nicht gelungen ist, auf die Beseitigung der hinreichend bekannten Mängel bei der derzeitigen Umsetzung der Grundsätze der „Safe-Harbour“-Vereinbarung hinzuwirken;

39. fordert die Kommission auf, Maßnahmen für die unverzügliche Aussetzung des Vollzugs der Entscheidung 2000/520/EG der Kommission, wonach die Grundsätze des „sicheren Hafens” angemessen sind, sowie der diesbezüglich vom Handelsministerium der USA vorgelegten „Häufig gestellten Fragen” vorzulegen; fordert die US-Behörden daher auf, einen Vorschlag über einen neuen Rahmen für die Übermittlung personenbezogener Daten aus der EU in die USA vorzulegen, der den Datenschutzanforderungen des EU-Rechts entspricht und das erforderliche angemessene Schutzniveau bietet;

40. fordert die zuständigen Behörden der Mitgliedstaaten, insbesondere die Datenschutzbehörden, auf, von ihren bestehenden Befugnissen Gebrauch zu machen, um die Datenübermittlung an Unternehmen, die sich öffentlich zur Einhaltung der Grundsätzen der „Safe-Harbour“-Vereinbarung mit den USA verpflichtet haben, unverzüglich auszusetzen, und zu verlangen, dass die Datenübermittlung an sie auf der Grundlage anderer Instrumente erfolgt und sofern diese die nötigen Sicherheits- und Garantiebestimmungen für den Schutz der Privatsphäre sowie der Grundrechte und Freiheiten von Personen enthalten;

41. fordert die Kommission auf, bis Dezember 2014 eine umfassende Bewertung des Rechtsrahmens der USA für den Schutz der Privatsphäre vorzulegen, die Handels-, Strafvollzugs- und Geheimdienstaktivitäten beurteilt, sowie in Anbetracht des Fehlens eines allgemeinen Datenschutzgesetzes in den Vereinigten Staaten konkrete Empfehlungen und Konsequenzen auszuarbeiten; bestärkt die Kommission darin, sich mit der US-Regierung auseinanderzusetzen, um einen Rechtsrahmen für ein hohes Schutzniveau von einzelnen Personen hinsichtlich des Schutzes ihrer personenbezogenen Daten, wenn diese in die USA übermittelt werden, zu schaffen und für die Gleichwertigkeit der in der EU und in den Vereinigten Staaten bestehenden rechtlichen Rahmenbedingungen für den Schutz der Privatsphäre zu sorgen;

Übermittlungen in andere Drittstaaten aufgrund von Entscheidungen über die Angemessenheit

42. erinnert daran, dass laut Richtlinie 95/46/EG Übermittlungen personenbezogener Daten in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen

Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig sind, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet, wobei mit dieser Bestimmung sichergestellt werden soll, dass der durch das EU-Datenschutzrecht gebotene Schutz auch bei der Übermittlung von Daten außerhalb der EU bestehen bleibt;

43. erinnert daran, dass laut Richtlinie 95/46/EG auch die Angemessenheit des Schutzniveaus, das ein Drittland bietet, unter Berücksichtigung aller Umstände beurteilt wird, die bei einer Datenübermittlung oder einer Kategorie solcher Übermittlungen eine Rolle spielen; erinnert zudem daran, dass die Kommission in der besagten Richtlinie auch mit Durchführungsbefugnissen ausgestattet wird, aufgrund derer sie feststellen kann, dass ein Drittland – gemessen an den Kriterien der Richtlinie 95/46/EG – ein angemessenes Schutzniveau gewährleistet; erinnert daran, dass die Kommission gemäß der Richtlinie 95/46/EG ebenfalls befugt ist, festzustellen, dass ein Drittland kein angemessenes Schutzniveau gewährleistet;

44. erinnert daran, dass die Mitgliedstaaten in letzterem Falle die erforderlichen Maßnahmen treffen müssen, damit keine gleichartige Datenübermittlung in das Drittland erfolgt, und dass die Kommission Verhandlungen einleiten sollte, um hier Abhilfe zu schaffen;

45. fordert die Kommission und die Mitgliedstaaten auf, unverzüglich zu prüfen, ob die in den Entscheidungen der Kommission 2013/65/EU vom 19. Januar 2012 bzw. 2002/2/EG vom 20. Dezember 2001 festgestellte Angemessenheit des Datenschutzniveaus, den der neuseeländische „Privacy Act“ und der kanadische „Personal Information Protection and Electronic Documents Act“ (Gesetz über personenbezogene Informationen und elektronische Dokumente) bieten, durch die Beteiligung der Geheimdienste dieser Länder an der Massenüberwachung von EU-Bürgern beeinträchtigt wurde, und erforderlichenfalls geeignete Maßnahmen zur Aussetzung des Vollzugs oder zur Aufhebung der Entscheidungen über die Angemessenheit zu ergreifen; fordert die Kommission außerdem dazu auf, die Situation in anderen Ländern zu prüfen, für die eine Angemessenheitsbewertung durchgeführt worden ist; erwartet von der Kommission, dass sie dem Parlament spätestens bis Dezember 2014 über ihre Erkenntnisse in Bezug auf die genannten Länder Bericht erstattet;

Übermittlungen auf der Grundlage von Vertragsklauseln und anderen Übereinkünften

46. erinnert daran, dass laut Angaben der nationalen Datenschutzbehörden weder Standardvertragsklauseln noch verbindliche unternehmensinterne Vorschriften in Hinblick auf den Zugriff auf personenbezogene Daten zu Massenüberwachungszwecken verfasst wurden und dass ein solcher Zugriff nicht den Ausnahmeklauseln zu den Vertragsklauseln oder verbindlichen unternehmensinternen Vorschriften entspreche, die sich auf außergewöhnliche Ausnahmen aus berechtigtem Interesse in einer demokratischen Gesellschaft, sofern erforderlich und angemessen, beziehen;

47. fordert die Mitgliedstaaten auf, Datenflüsse in Drittstaaten auf der Grundlage der von den zuständigen nationalen Behörden genehmigten Standardvertragsklauseln,

Vertragsklauseln oder bindenden unternehmensinternen Vorschriften zu untersagen bzw. einzustellen, wenn wahrscheinlich ist, dass die Datenempfänger nach den für sie geltenden Rechtsvorschriften Anforderungen unterliegen, die über die in einer demokratischen Gesellschaft unbedingt erforderlichen, angemessenen und verhältnismäßigen Beschränkungen hinausgehen und sich wahrscheinlich nachteilig auf die Garantien auswirken werden, die das anwendbare Datenschutzrecht und die Standardvertragsklauseln bieten, oder wenn die Fortsetzung der Datenübermittlung den betroffenen Personen einen schweren Schaden zuzufügen droht;

48. fordert die Artikel-29-Arbeitsgruppe auf, Leitlinien und Empfehlungen zu den Garantien und Schutzmaßnahmen herauszugeben, die in den Vertragswerken für internationale Übermittlungen personenbezogener Daten aus der EU enthalten sein sollten, um den Datenschutz sowie den Schutz der Grundrechte und Grundfreiheiten des Einzelnen sicherzustellen, wobei insbesondere die Gesetze der Drittstaaten zu Nachrichtendiensten und nationaler Sicherheit sowie die Beteiligung der Unternehmen, die die Daten in einem Drittstaat erhalten, an Massenüberwachungsaktivitäten von Nachrichtendiensten eines Drittstaats berücksichtigt werden sollen;

49. fordert die Kommission auf, unverzüglich die aufgestellten Standardvertragsklauseln zu prüfen, um zu beurteilen, ob sie hinsichtlich des Zugriffs auf gemäß den Klauseln übermittelte personenbezogene Daten zu nachrichtendienstlichen Zwecken den erforderlichen Schutz bieten, und sie gegebenenfalls zu überarbeiten;

Übermittlungen auf Grundlage des Rechtshilfeabkommens

50. fordert die Kommission auf, vor Ende 2014 eine eingehende Beurteilung des bestehenden Rechtshilfeabkommens gemäß Artikel 17 durchzuführen, um dessen praktische Umsetzung zu prüfen und dabei insbesondere festzustellen, ob die USA von dem Abkommen tatsächlich Gebrauch gemacht haben, um Informationen oder Nachweise in der EU einzuholen, und ob das Abkommen umgangen wurde, um die Informationen direkt in der EU zu erhalten, und außerdem die Auswirkungen auf die Grundrechte des Einzelnen zu beurteilen; eine solche Beurteilung sollte sich nicht nur auf amtliche Feststellungen der USA als ausreichende Grundlage für die Analyse berufen, sondern auch auf bestimmten Auswertungen der EU basieren; bei dieser eingehenden Prüfung sollten auch die Folgen der Anwendung der konstitutionellen Architektur der Europäischen Union auf diesen Rechtsakt behandelt werden, um eine Anpassung an Unionsrecht vorzunehmen, wobei insbesondere das Protokoll 36 und dessen Artikel 10 sowie die Erklärung 50 zu diesem Protokoll zu berücksichtigen sind; fordert den Rat und die Kommission ferner auf, die bilateralen Abkommen zwischen den Mitgliedstaaten und den USA auszuwerten, um die Kohärenz zwischen diesen bilateralen Abkommen und den bestehenden oder künftigen Abkommen der EU mit den USA sicherzustellen;

EU-Rechtshilfe in Strafsachen

51. ersucht den Rat und die Kommission, das Parlament darüber zu informieren, inwiefern das Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten, insbesondere dessen Titel III zur Überwachung des

Telekommunikationsverkehrs, von den Mitgliedstaaten tatsächlich angewandt wird; fordert die Kommission auf, wie beantragt vor Ende 2014 in Übereinstimmung mit der Erklärung 50 zum Protokoll 36 einen Vorschlag vorzulegen, um eine Anpassung an den Rahmen des Vertrags von Lissabon vorzunehmen;

Übermittlungen auf der Grundlage der TFTP- und PNR-Abkommen

52. vertritt die Ansicht, dass aus den von der Kommission und dem US-Finanzministerium bereitgestellten Informationen nicht klar hervorgeht, ob US-Nachrichtendienste auf SWIFT-Finanznachrichten in der EU zugreifen können, indem sie allein oder in Zusammenarbeit mit nationalen Nachrichtendiensten der EU und ohne auf bestehende bilaterale Kanäle für Rechtshilfe und justizielle Zusammenarbeit zurückzugreifen, SWIFT-Netze oder Betriebssysteme bzw. Kommunikationsnetze von Banken abfangen;

53. bekräftigt seine Entschließung vom 23. Oktober 2013 und fordert die Kommission auf, das TFTP-Abkommen auszusetzen;

54. fordert die Kommission auf, auf Bedenken in Bezug auf die Tatsache zu reagieren, dass drei der größten von Fluggesellschaften weltweit genutzten computerisierten Reservierungssysteme in den USA ansässig sind und PNR-Daten in Cloud-Systemen gespeichert werden, die auf US-amerikanischem Boden nach US-amerikanischem Recht betrieben werden, wodurch kein ausreichender Datenschutz gegeben ist;

Rahmenvereinbarung zum Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit („Rahmenabkommen")

55. vertritt die Auffassung, dass eine zufriedenstellende Lösung unter dem „Rahmenabkommen" eine Vorabbedingung für die vollständige Wiederherstellung des Vertrauens zwischen den transatlantischen Partnern darstellt;

56. fordert die umgehende Wiederaufnahme der Verhandlungen mit den USA zu dem „Rahmenabkommen", das EU-Bürgern die gleichen Rechte wie US-Bürgern einräumen sollte; betont, dass dieses Abkommen überdies gültige und durchsetzbare administrative und gerichtliche Rechtsbehelfe für alle EU-Bürger in den USA ohne jegliche Diskriminierung gewährleisten sollte;

57. fordert die Kommission und den Rat auf, keine neuen sektoralen Vereinbarungen oder Regelungen zur Übermittlung personenbezogener Daten zu Strafverfolgungszwecken mit den USA zu treffen, solange das „Rahmenabkommen" nicht in Kraft getreten ist;

58. fordert die Kommission dringend auf, bis April 2014 ausführlich über die verschiedenen Punkte des Verhandlungsmandats und den aktuellen Stand zu berichten;

Datenschutzreform

59. fordert den Vorsitz im Rat und die Mitgliedstaaten auf, ihre Arbeiten am gesamten Datenschutzpaket voranzutreiben, sodass seine Annahme im Jahr 2014 ermöglicht

wird, damit die EU-Bürger in sehr naher Zukunft von einem hohen Datenschutzniveau profitieren können; betont, dass ein entschlossenes Handeln und die volle Unterstützung durch den Rat notwendige Voraussetzungen sind, um Glaubwürdigkeit und Durchsetzungskraft gegenüber Drittstaaten zu demonstrieren;

60. betont, dass sowohl die Datenschutzverordnung als auch die Datenschutzrichtlinie zum Schutz der Grundrechte des Einzelnen notwendig sind und dass daher beide als gleichzeitig zu verabschiedendes Paket behandelt werden müssen, um sicherzustellen, dass bei allen Datenverarbeitungsaktivitäten in der EU unter allen Umständen ein hohes Schutzniveau geboten wird; betont, dass es nur dann weitere Maßnahmen für die Zusammenarbeit im Bereich der Strafverfolgung ergreifen wird, nachdem der Rat Verhandlungen über das Datenschutzpaket mit dem Parlament und der Kommission aufgenommen hat;

61. erinnert daran, dass die Grundsätze des „eingebauten Datenschutzes“ (privacy by design) und der „datenschutzfreundlichen Voreinstellungen“ (privacy by default) eine Stärkung des Datenschutzes darstellen und für alle Produkte, Dienste und Systeme, die im Internet angeboten werden, den Status einer Richtschnur haben sollten;

62. ist der Auffassung, dass mehr Transparenz und höhere Sicherheitsstandards für Online- und Telekommunikationsdienste von grundlegender Bedeutung für die Erreichung verbesserter Datenschutzregelungen sind; fordert die Kommission daher auf, einen Legislativvorschlag zu standardisierten allgemeinen Geschäftsbedingungen für Online- und Telekommunikationsdienste vorzulegen und eine Aufsichtsbehörde mit der Überwachung der Einhaltung der allgemeinen Geschäftsbedingungen zu beauftragen;

Cloud Computing

63. bemerkt, dass sich die oben genannten Vorgehensweisen negativ auf das Vertrauen in das US-Cloud-Computing und die US-Cloud-Anbieter ausgewirkt haben; hebt daher die Entwicklung europäischer Clouds und IT-Lösungen als wesentliches Element für Wachstum und Beschäftigung sowie für das Vertrauen in Cloud-Computing-Dienste und -Anbieter sowie für die Sicherung eines hohen Schutzniveaus für personenbezogene Daten hervor;

64. fordert alle öffentlichen Einrichtungen in der Union auf, in Fällen, in denen Nicht-EU-Gesetze greifen, keine Cloud-Dienste zu verwenden;

65. bekräftigt seine ernsthaften Bedenken bezüglich der verbindlichen direkten Weitergabe personenbezogener Daten und Informationen aus der EU an Behörden in Drittstaaten im Rahmen von Cloud-Verträgen durch Cloud-Anbieter, die dem Recht eines Drittstaates unterstehen oder Server zur Speicherung in Drittstaaten verwenden, sowie auch bezüglich des direkten Fernzugriffs auf personenbezogene Daten und Informationen durch die Strafverfolgungsbehörden und Nachrichtendienste von Drittstaaten;

66. bedauert, dass die Behörden von Drittstaaten gewöhnlich in direkter Durchsetzung eigener Rechtsvorschriften auf die Daten zugreifen, ohne sich der internationalen

Rechtsakte zur rechtlichen Zusammenarbeit, wie z. B. Rechtshilfeabkommen oder anderer Formen der justiziellen Zusammenarbeit, zu bedienen;

67. appelliert an die Kommission und die Mitgliedstaaten, die Arbeit an der Europäischen Cloud-Partnerschaft zu beschleunigen und dabei die Zivilgesellschaft und die technische Gemeinschaft, wie beispielsweise die Internet Engineering Task Force (IETF), umfassend einzubeziehen sowie Datenschutzaspekte zu berücksichtigen;

68. fordert die Kommission nachdrücklich auf, bei der Aushandlung internationaler Abkommen, die die Verarbeitung personenbezogener Daten berühren, die mit dem „Cloud-Computing“ verbundenen Risiken und Herausforderungen für die Grundrechte, insbesondere, aber nicht ausschließlich, für das Recht auf Privatsphäre und den Schutz personenbezogener Daten gemäß Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union, besonders zu berücksichtigen; fordert die Kommission zudem auf, die innerstaatlichen Vorschriften des Verhandlungspartners über den Zugang zu personenbezogenen Daten, die über „Cloud-Computing“-Dienste verarbeitet werden, zum Zwecke der Strafverfolgung und nachrichtendienstlicher Tätigkeiten zu berücksichtigen, insbesondere die Bedingung, dass sie nur im Rahmen eines rechtmäßigen Verfahrens zu solchen Daten Zugang erhalten dürfen und dass es einer eindeutigen Rechtsgrundlage für den Zugang bedarf, sowie die Bedingung, die genauen Zugangsvoraussetzungen, den Zweck eines solchen Zugangs, die bei der Datenübergabe zu ergreifenden Sicherheitsmaßnahmen, die Rechte des Einzelnen sowie die Vorschriften für die Überwachung und für ein wirksames Rechtsbehelfsverfahren festzulegen;

69. weist darauf hin, dass alle Unternehmen, die in der EU Dienstleistungen anbieten, ausnahmslos die Rechtsvorschriften der EU einhalten und für etwaige Rechtsverstöße haften müssen; unterstreicht zudem die Notwendigkeit, über wirksame, verhältnismäßige und abschreckende verwaltungsrechtliche Sanktionen zu verfügen, die Cloud-Computing-Anbietern auferlegt werden können, die nicht im Einklang mit den Datenschutzstandards der EU handeln;

70. fordert die Kommission und die zuständigen Behörden der Mitgliedstaaten auf, zu prüfen, in welchem Ausmaß die EU-Regelungen zur Privatsphäre und zum Datenschutz durch die Zusammenarbeit der Rechtsträger der EU mit den Geheimdiensten bzw. durch die Anerkennung richterlicher Anordnungen von Behörden aus Drittstaaten zur Herausgabe personenbezogener Daten von EU-Bürgern entgegen der Datenschutzgesetzgebung der EU verletzt wurden;

71. fordert die Anbieter neuer Dienste auf der Grundlage von „Big Data“ sowie neuer Anwendungen, wie beispielsweise „das Internet der Dinge“, dazu auf, bereits während der Entwicklungsphase Datenschutzmaßnahmen zu berücksichtigen, um ein hohes Maß an Vertrauen der Bürger aufrecht zu erhalten;

Abkommen über die transatlantische Handels- und Investitionspartnerschaft (TTIP)

72. stellt fest, dass die EU und die USA Verhandlungen über eine transatlantische Handels- und Investitionspartnerschaft führen, die von großer strategischer Bedeutung für weiteres Wirtschaftswachstum ist;

73. hebt angesichts der Bedeutung der digitalen Wirtschaft in den Beziehungen und bei der Wiederherstellung des Vertrauens zwischen der EU und den USA besonders hervor, dass die Zustimmung des Europäischen Parlaments zu dem endgültigen TTIP-Abkommen gefährdet sein könnte, solange die pauschale Massenüberwachung sowie das Abfangen von Nachrichten in EU-Institutionen und diplomatischen Vertretungen nicht völlig eingestellt werden und keine angemessene Lösung für Datenschutzrechte von EU-Bürgern, einschließlich behördlicher und gerichtlicher Rechtsbehelfe, gefunden wird; betont, dass das Parlament dem endgültigen TTIP-Abkommen nur zustimmen kann, wenn u.a. darin die von der EU-Charta anerkannten Grundrechte in vollem Umfang respektiert werden und insofern der Schutz der Privatsphäre des Einzelnen im Zusammenhang mit der Verarbeitung und Verbreitung personenbezogener Daten weiterhin durch Artikel XIV des GATS geregelt werden; betont, dass die Datenschutzgesetzgebung der EU im Rahmen der Anwendung von Artikel XIV des GATS nicht als „willkürliche oder ungerechtfertigte Diskriminierung“ erachtet werden kann;

Demokratische Aufsicht über Nachrichtendienste

74. betont, dass die Aufsicht über die Tätigkeiten der Nachrichtendienste zwar sowohl auf demokratischer Legitimität (starker Rechtsrahmen, Ex-ante-Genehmigung und Ex-post-Überprüfung) als auch auf angemessenen technischen Fähigkeiten und Kenntnissen basieren sollte, es den meisten derzeitigen Aufsichtsgremien in der EU und den USA jedoch erheblich an beidem, insbesondere an den technischen Fähigkeiten, mangelt;

75. fordert wie im Falle von Echelon alle nationalen Parlamente, die dies noch nicht getan haben, auf, eine effektive Aufsicht über die Nachrichtendienstaktivitäten durch Parlamentarier oder Sachverständigengremien mit Untersuchungsvollmachten einzurichten; ruft die nationalen Parlamente auf, sicherzustellen, dass diese Aufsichtsausschüsse/-gremien über ausreichende Ressourcen, technische Kenntnisse und Rechtsmittel, einschließlich des Rechts, Besichtigungen vor Ort durchzuführen, für eine effektive Kontrolle der Nachrichtendienste verfügen;

76. fordert die Bildung einer hochrangigen Gruppe, die in transparenter Weise und in Zusammenarbeit mit den Parlamenten Empfehlungen und weitere Schritte für eine stärkere demokratische Aufsicht, einschließlich der parlamentarischen Aufsicht, über die Nachrichtendienste auf EU-Ebene, und eine stärkere Zusammenarbeit in der EU im Bereich der Aufsicht, insbesondere hinsichtlich der grenzüberschreitenden Dimension, vorschlagen soll;

77. Diese hochrangige Gruppe sollte:

- europäische Mindestnormen oder Leitlinien zur (Ex-ante- und Ex-post)-Aufsicht der Nachrichtendienste auf der Grundlage bestehender bewährter Methoden und Empfehlungen internationaler Gremien (UN, Europarat) definieren, einschließlich des Problems, dass Aufsichtsgremien nicht als dritte Partei im Sinne der „Drittparteiregel“ oder des Grundsatzes der „Kontrolle durch den Urheber“ gelten, sowie zur Aufsicht und Rechenschaftspflicht ausländischer Nachrichtendienste;

- die Dauer und die Reichweite jeder angeordneten Überwachung strikt begrenzen, sofern deren Fortsetzung nicht ordnungsgemäß durch die Genehmigungs-/Aufsichtsbehörde begründet wird; in Erinnerung rufen, dass die Dauer jeder angeordneten Überwachung verhältnismäßig und auf ihren Zweck begrenzt sein sollte;

- Kriterien für mehr Transparenz auf der Grundlage des allgemeinen Grundsatzes des Zugangs zu Informationen und der sogenannten „Tshwane-Prinzipien“[1] erarbeiten;

78. beabsichtigt, bis Ende 2014 eine Konferenz mit nationalen — parlamentarischen und unabhängigen — Aufsichtsgremien zu organisieren;

79. fordert die Mitgliedstaaten auf, auf bewährte Methoden zurückzugreifen, um den Zugang ihrer Aufsichtsgremien zu Informationen bezüglich Nachrichtendienstaktivitäten (einschließlich Verschlusssachen und Informationen von anderen Diensten) zu verbessern und für die Befugnis zu Besichtigungen vor Ort, umfassende Befragungsbefugnisse, angemessene Ressourcen und technische Kenntnisse, völlige Unabhängigkeit von den jeweiligen Regierungen sowie eine Meldepflicht gegenüber den jeweiligen Parlamenten zu sorgen;

80. fordert die Mitgliedstaaten auf, die Zusammenarbeit der Aufsichtsgremien untereinander auszubauen, insbesondere innerhalb des European Network of National Intelligence Reviewers (ENNIR — europäisches Expertennetz zur Kontrolle der Nachrichtendienste);

81. fordert die Kommission und die Hohe Vertreterin/Vizepräsidentin der Kommission dringend auf, bis Dezember 2014 einen Vorschlag für eine Rechtsgrundlage für die Tätigkeit des EU-Zentrums für Informationsgewinnung und -analyse (IntCen) zusammen mit einem geeigneten Aufsichtsmechanismus vorzulegen; fordert die Hohe Vertreterin/Vizepräsidentin der Kommission dringend dazu auf, gegenüber den verantwortlichen Organen des Parlaments regelmäßig Rechenschaft über die Tätigkeit des EU-Zentrums für Informationsgewinnung und -analyse (IntCen) abzulegen, unter anderem auch über die vollständige Wahrung der grundlegenden Menschenrechte und die Einhaltung der jeweils anwendbaren Datenschutzbestimmungen der EU, und mit dem Parlament seinen bestehenden Aufsichtsmechanismus besonders zu erläutern;

82. fordert die Kommission auf, bis Dezember 2014 einen Vorschlag für ein EU-Verfahren der Sicherheitsüberprüfung für alle EU-Amtsträger vorzulegen, da das aktuelle System, das auf der vom Mitgliedstaat der Staatsangehörigkeit durchgeführten Sicherheitsüberprüfung beruht, unterschiedliche Anforderungen und Verfahrensdauer innerhalb nationaler Systeme ermöglicht und somit zu einer unterschiedlichen Behandlung von Parlamentsmitgliedern und ihren Mitarbeitern je nach Staatsangehörigkeit führt;

83. erinnert an die Bestimmungen der Interinstitutionellen Vereinbarung zwischen dem Parlament und dem Rat über die Übermittlung an und die Bearbeitung durch das Europäische Parlament von im Besitz des Rates befindlichen Verschlusssachen in Bezug auf Angelegenheiten, die nicht unter die Gemeinsame Außen- und Sicherheitspolitik fallen, welche zur Verbesserung der Aufsicht auf EU-Ebene

[1] Die weltweiten Prinzipien zur nationalen Sicherheit und dem Recht auf Informationen, Juni 2013.

verwendet werden sollten;

EU-Agenturen

84. fordert die Gemeinsame Kontrollinstanz von Europol auf, zusammen mit nationalen Datenschutzbehörden vor Ende 2014 eine gemeinsame Inspektion durchzuführen, um festzustellen, ob Informationen und personenbezogene Daten, die an Europol weitergegeben wurden, rechtmäßig von nationalen Behörden erworben wurden, und insbesondere, ob die Informationen bzw. Daten ursprünglich von Nachrichtendiensten in der EU oder einem Drittstaat erworben wurden und ob entsprechende Maßnahmen getroffen wurden, um die Nutzung und weitere Verbreitung solcher Informationen oder Daten zu verhindern; vertritt die Auffassung, dass Europol keine Informationen oder Daten verarbeiten sollte, die unter Verletzung der in der Charta der Grundrechte verbürgten Grundrechte beschafft wurden;

85. fordert Europol auf, von seinem Mandat umfassend Gebrauch zu machen und die zuständigen Behörden der Mitgliedstaaten zu ersuchen, strafrechtliche Ermittlungen zu größeren Cyberangriffen und IT-Verstößen mit möglichen grenzüberschreitenden Auswirkungen einzuleiten; ist der Ansicht, dass das Mandat von Europol ausgeweitet werden sollte, um ihm zu ermöglichen, seine eigenen Untersuchungen aufgrund des Verdachts eines böswilligen Angriffs auf das Netz und die Informationssysteme von zwei oder mehr Mitgliedstaaten oder Organen der Union einzuleiten[1]; fordert die Kommission auf, die Aktivitäten des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität zu überprüfen und, falls erforderlich, einen Vorschlag für ein umfassendes Rahmenwerk zur Stärkung seiner Zuständigkeiten vorzulegen;

Recht auf freie Meinungsäußerung

86. äußert seine tiefe Sorge angesichts der zunehmenden Bedrohungen der Pressefreiheit und die sich aus der Einschüchterung durch staatliche Behörden ergebende abschreckende Wirkung auf Journalisten, insbesondere in Hinblick auf die Wahrung der Vertraulichkeit journalistischer Quellen; bekräftigt die Aufrufe aus seiner Entschließung vom 21. Mai 2013 zur „EU-Charta: Normensetzung für die Freiheit der Medien in der EU“;

87. nimmt die Festnahme von David Miranda und die Beschlagnahme des in dessen Besitz befindlichen Materials auf Grundlage von Anhang 7 des UK Terrorism Act 2000 (sowie die Aufforderung an *The Guardian*, das Material zu vernichten oder auszuhändigen) zur Kenntnis und zeigt sich besorgt, dass dies eine mögliche gravierende Beeinträchtigung des Rechts der freien Meinungsäußerung und der Medienfreiheit gemäß Artikel 10 EMRK und Artikel 11 der EU-Charta darstellt und dass Rechtsvorschriften, die eigentlich zur Bekämpfung des Terrorismus gedacht sind, in solchen Fällen missbraucht werden können;

[1] Legislative Entschließung des Europäischen Parlaments vom...Februar 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für die Zusammenarbeit und die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (Europol) (A7-0096/2014)

88. macht auf die schwierige Lage von Informanten und ihrer Unterstützer, einschließlich von Journalisten, im Anschluss an ihre Enthüllungen aufmerksam; fordert die Kommission auf, eine Untersuchung durchzuführen, ob ein künftiger Gesetzesvorschlag zur Einrichtung eines wirksamen und umfassenden europäischen Programms für den Schutz von Informanten, wie es bereits in der Entschließung des Parlaments vom 23. Oktober gefordert wurde, auch andere Zuständigkeitsbereiche der Union unter besonderer Berücksichtigung der Komplexität des „Whistleblowing“ im Bereich der Nachrichtendienste umfassen sollte; fordert die Mitgliedstaaten zu einer eingehenden Prüfung der Möglichkeit auf, Informanten internationalen Schutz vor strafrechtlicher Verfolgung zu gewähren;

89. fordert die Mitgliedstaaten auf, dafür Sorge zu tragen, dass ihre Rechtsvorschriften, insbesondere auf dem Gebiet der nationalen Sicherheit, eine sichere Alternative für das Verschweigen der Aufdeckung von oder der Berichterstattung über Fehlverhalten bieten, einschließlich Korruption, Straftaten, Verstöße gegen rechtliche Verpflichtungen, Justizirrtümer und Amtsmissbrauch, was auch im Einklang mit den Bestimmungen verschiedener internationaler (UNO und Europarat) Instrumente zur Bekämpfung von Korruption, den in der Entschließung 1729 (2010) der Parlamentarischen Versammlung des Europarates niedergelegten Grundsätzen, den „Tshwane-Prinzipien“ usw. steht;

IT-Sicherheit in der EU

90. weist darauf hin, dass die jüngsten Ereignisse die extreme Anfälligkeit der EU, insbesondere der Gemeinschaftsorgane, nationalen Regierungen und Parlamente, wichtigen europäischen Unternehmen, der europäischen IT-Infrastrukturen und Netzwerke, gegenüber technisch ausgereiften Angriffen mit komplexer Software und Malware deutlich machen; stellt fest, dass für diese Angriffe eine finanzielle und personelle Ausstattung in einem solchen Umfang erforderlich ist, dass sie wahrscheinlich von staatlichen Einrichtungen im Auftrag von ausländischen Regierungen ausgehen; versteht in diesem Zusammenhang den Hacking- und Spähangriff auf das Telekommunikationsunternehmen Belgacom als besorgniserregendes Beispiel eines Angriffs auf die IT-Kapazitäten der EU; hebt hervor, dass ein höheres Maß an IT-Kapazität und -Sicherheit der EU auch die Anfälligkeit der EU gegenüber gravierenden Cyberangriffen, die von großen kriminellen Organisationen oder Terroristengruppen ausgehen, verringert;

91. vertritt die Auffassung, dass die Enthüllungen über die Massenüberwachung, die diese Krise ausgelöst haben, von Europa als Chance genutzt werden können, die Initiative zu ergreifen und als strategische prioritäre Maßnahme starke und autonome IT-Schlüsselkapazitäten aufzubauen; hebt hervor, dass für die Wiederherstellung von Vertrauen diese europäischen IT-Kapazitäten möglichst auf offenen Standards sowie auf quelloffener Software und, wenn möglich, Hardware basieren müssen, wodurch die gesamte Lieferkette – vom Prozessordesign bis hin zur Anwendungsebene – transparent und überprüfbar wird; weist darauf hin, dass ein digitaler „New Deal” erforderlich ist, in dessen Rahmen sich EU-Institutionen, Mitgliedstaaten, Forschungsinstitute, Unternehmen und Zivilgesellschaft gemeinsam durch umfassende Maßnahmen für eine Wiederbelebung der Wettbewerbsfähigkeit in dem strategisch

wichtigen IT-Sektor einsetzen; ruft die Kommission und die Mitgliedstaaten auf, das öffentliche Auftragswesen als Druckmittel für die Unterstützung solcher Schlüsselkapazitäten in der EU zu nutzen und die Sicherheits- und Datenschutzbestimmungen der EU zu einer entscheidenden Anforderung bei der öffentlichen Beschaffung von IT-Waren und -Dienstleistungen zu machen; fordert die Kommission daher dringend dazu auf, die derzeitigen Praktiken beim öffentlichen Auftragswesen mit Blick auf die Datenverarbeitung zu überprüfen und in Betracht zu ziehen, die Ausschreibungen auf zertifizierte Unternehmen und gegebenenfalls auf EU-Unternehmen zu beschränken, falls Sicherheitsinteressen oder andere wichtige Interessen berührt sind;

92. verurteilt aufs Schärfste die Tatsache, dass Geheimdienste versucht haben, die IT-Sicherheitsstandards zu senken und „Backdoors“ („Hintertüren“) in vielen verschiedenen IT-Systemen zu installieren; fordert die Kommission auf, einen Gesetzesentwurf für das Verbot der Verwendung von „Backdoors“ durch Strafverfolgungsbehörden vorzulegen; empfiehlt folglich die Verwendung von quelloffener Software in allen Umgebungen, in denen die IT-Sicherheit eine wichtige Rolle spielt;

93. fordert alle Mitgliedstaaten, die Kommission, den Rat und den Europäischen Rat auf, ihre vollste Unterstützung, einschließlich Finanzierung im Bereich Forschung und Entwicklung, für die Entwicklung von europäischen innovativen und technischen Kapazitäten in Bezug auf IT-Instrumente, -Unternehmen und -Anbieter (Hardware, Software, Dienstleistungen und Netze), einschließlich zu Zwecken der Cybersicherheit, sowie Verschlüsselungskapazitäten und kryptografischer Möglichkeiten, zu gewähren;

94. fordert die Kommission, Normungsgremien und ENISA auf, bis Dezember 2014, Mindeststandards für Sicherheit und Datenschutz und Leitlinien für IT-Systeme, -Netzwerke und -Dienste, einschließlich Cloud-Computing-Diensten, zu entwickeln, um die persönlichen Daten der EU-Bürgerinnen und -Bürger sowie die Integrität aller IT-Systeme besser zu schützen; ist der Überzeugung, dass diese Standards, die zum Maßstab für neue weltweite Standards werden könnten, eher in einem offenen und demokratischen Verfahren festgelegt werden sollten als von einem einzelnen Land, einer einzelnen Einrichtung oder einem multinationalen Unternehmen vorangetrieben zu werden; vertritt die Ansicht, dass berechtigte Interessen der Strafverfolgung und Geheimdienste zwar berücksichtigt werden müssen, um den Kampf gegen den Terrorismus zu unterstützen, dass dies jedoch nicht zu einer generellen Aushöhlung der Zuverlässigkeit aller IT-Systeme führen darf; bekundet seine Unterstützung für die kürzlich getroffene Entscheidung der Internet Engineering Task Force (IETF), auch Regierungen in das Bedrohungsmodell für Internetsicherheit aufzunehmen;

95. weist darauf hin, dass die EU sowie nationale Regulierungsbehörden für Telekommunikation und in bestimmten Fällen auch Telekommunikationsunternehmen die IT-Sicherheit ihrer Nutzer und Kunden eindeutig vernachlässigt haben; fordert die Kommission auf, ihre bestehenden Befugnisse im Rahmen der Datenschutzrichtlinie für elektronische Kommunikation und Telekommunikation in vollem Umfang zu nutzen, um den Schutz der Vertraulichkeit von Kommunikation durch Maßnahmen zu

verbessern, mit denen sichergestellt wird, dass Endgeräte in einer Weise gebaut sind, die mit dem Recht der Nutzer auf Schutz und Kontrolle der Verwendung ihrer personenbezogenen Daten vereinbar ist, und um für ein hohes Maß an Sicherheit bei Telekommunikationsnetzen und -diensten zu sorgen, u.a. indem eine hochmoderne und durchgängige Verschlüsselung der Kommunikation gefordert wird;

96. unterstützt die Cybersicherheitsstrategie der EU; ist jedoch der Ansicht, dass diese nicht alle potenziellen Bedrohungen abdeckt und dass sie auf gefährliches Verhalten von Staaten ausgedehnt werden sollte; betont die Notwendigkeit einer robusteren IT-Sicherheit sowie einer stärkeren Belastbarkeit der IT-Systeme;

97. fordert die Kommission auf, bis spätestens Januar 2015 einen Aktionsplan vorzulegen, um eine größere Unabhängigkeit der EU im IT-Sektor zu schaffen, einschließlich eines kohärenteren Ansatzes für den Ausbau der europäischen technischen IT-Kapazitäten (inklusive IT-Systemen, Geräten, Diensten, Cloud-Computing, Verschlüsselung und Anonymisierung) und für den Schutz wesentlicher IT-Infrastrukturen (auch hinsichtlich Eigentum und Schwachstellen);

98. fordert die Kommission auf, im nächsten Arbeitsprogramm des Rahmenprogramms „Horizont 2020“ mehr Mittel für die Förderung der europäischen Forschung, Entwicklung, Innovation und Schulung im Bereich der IT-Technologien einzusetzen, vor allem für Technologien und Infrastrukturen für einen besseren Datenschutz, Verschlüsselung, sichere Datenverarbeitung, quelloffene Sicherheitslösungen und andere Dienstleistungen für die Informationsgesellschaft, sowie auch den Binnenmarkt für europäische Soft- und Hardware und verschlüsselte Kommunikationsmittel und Kommunikationsinfrastrukturen voranzutreiben, einschließlich durch Auflegung einer umfassenden EU-Industriestrategie für die IT-Industrie; vertritt die Auffassung, dass kleine und mittlere Unternehmen bei der Forschung eine besondere Rolle spielen; betont, dass keine EU-Mittel für Projekte bereitgestellt werden sollten, die nur dazu dienen, Instrumente zu entwickeln, um einen illegalen Zugang zu IT-Systemen zu erreichen;

99. fordert die Kommission auf, die gegenwärtigen Zuständigkeiten im Einzelnen festzulegen und bis spätestens Dezember 2014 den Bedarf für ein umfassenderes Mandat, eine bessere Koordination und/oder zusätzliche Mittel und technische Kapazitäten für ENISA, das Europäische Zentrum zur Bekämpfung der Cyberkriminalität von Europol, und andere einschlägig spezialisierte Kompetenzzentren der Union, CERT-EU und den EDSB zu prüfen, damit diese eine Schlüsselrolle bei der Sicherung der europäischen Kommunikationssysteme spielen, gravierende Verletzungen der IT-Sicherheit in der EU wirksamer verhindern und untersuchen und technische Untersuchungen im Zusammenhang mit gravierenden Verletzungen vor Ort durchführen (oder Mitgliedstaaten und EU-Organe bei der Durchführung unterstützen) können; fordert die Kommission insbesondere auf, in Betracht zu ziehen, die Rolle von ENISA beim Schutz der internen Systeme der EU-Organe zu stärken und ein Notfallteam mit entsprechender Zuständigkeit (Computer Emergency Response Team, CERT) für die EU und ihre Mitgliedstaaten in die ENISA einzugliedern;

100. ersucht die Kommission, die Notwendigkeit einer eigenen IT-Akademie zu prüfen, in der die besten unabhängigen europäischen und internationalen Fachleute auf allen damit zusammenhängenden Fachgebieten zusammengeführt werden und die Aufgabe erhalten, alle einschlägigen Gemeinschaftsorganen und -einrichtungen zu IT-Technologien, u.a. zu sicherheitsbezogenen Strategien, wissenschaftlich zu beraten;

101. fordert die zuständigen Dienststellen des Generalsekretariats des Europäischen Parlaments auf, unter der Verantwortung des Präsidenten des Parlaments bis spätestens Dezember 2014 eine gründliche Prüfung und Bewertung der Zuverlässigkeit der IT-Sicherheit des Europäischen Parlaments mit Schwerpunkt auf Folgendem durchzuführen: Haushaltsmittel, personelle Ausstattung, technische Kapazitäten, interne Organisation und alle relevanten Elemente, um bei den IT-Systemen des Parlaments ein hohes Maß an Sicherheit zu erreichen; ist der Auffassung, dass eine solche Bewertung mindestens Informationen, Analyse und Empfehlungen zu folgenden Themen umfassen muss:

- der Bedarf an regelmäßigen, strengen und unabhängigen Sicherheitsüberprüfungen und Penetrationstests, mit der Auswahl externer Sicherheitsfachleute, um Transparenz und deren Legitimation gegenüber Drittländern oder anderen Interessengruppen sicherzustellen;

- die Einbeziehung bestimmter IT-Sicherheits-/Datenschutzanforderungen bei Ausschreibungsverfahren für neue IT-Systeme, u.a. die Möglichkeit, quelloffene Software als Kaufbedingung einzubeziehen, oder eine Vorgabe, dass sich vertrauenswürdige europäische Unternehmen an der Ausschreibung beteiligen sollten, wenn sensible sicherheitsrelevante Bereiche betroffen sind;

- die Liste der Unternehmen, die beim Europäischen Parlament im IT- und Telekommunikationsbereich unter Vertrag stehen, unter Berücksichtigung sämtlicher Informationen, die über deren Zusammenarbeit mit Geheimdiensten ans Licht gekommen sind (wie die Enthüllungen über NSA-Verträge mit einem Unternehmen wie RSA, dessen Produkte das Europäische Parlament eigentlich dafür nutzt, den Fernzugriff durch Abgeordnete und Mitarbeiter auf seine Datenbank zu schützen), einschließlich der Möglichkeit, dass dieselben Dienstleistungen von anderen, vorzugsweise europäischen, Unternehmen erbracht werden;

- die Zuverlässigkeit und Belastbarkeit von Software, und insbesondere von serienmäßig produzierter kommerzieller Software, die von den Gemeinschaftsorganen in ihren IT-Systemen verwendet wird, in Bezug auf das Eindringen von Strafverfolgungs- und Geheimdienstbehörden der EU oder von Drittländern, auch unter Berücksichtigung einschlägiger internationaler Normen, Grundsätzen der besten Praxis für das Management von Sicherheitsrisiken und der Einhaltung der EU-Normen für die Netz- und Informationssicherheit bei Sicherheitsverletzungen;

- die Verwendung von mehr quelloffenen Systemen;

- Schritte und Maßnahmen, um den verstärkten Einsatz von mobilen Geräten (z. B. Smartphones, Tablets, unabhängig vom beruflichen oder privaten Gebrauch) und dessen Auswirkungen auf die IT-Sicherheit des Systems anzugehen;

- die Sicherheit der Kommunikation zwischen den verschiedenen Arbeitsorten des Parlaments und der im Parlament genutzten IT-Systeme;

- die Verwendung und die Standorte von Servern und IT-Zentren für das IT-System des Parlaments und deren Bedeutung für die Sicherheit und Integrität der Systeme;

- die praktische Umsetzung der geltenden Vorschriften für Sicherheitsverletzungen und die umgehende Benachrichtigung der zuständigen Behörden durch den Anbieter öffentlicher Kommunikationsnetze;

- die Verwendung von Cloud-Computing und Speicheranlagen durch das Parlament, einschließlich der in der Cloud gesicherten Arten von Daten, wie die Inhalte und der Zugriff geschützt sind und wo sich die Cloud-Server befinden, um den für den Datenschutz und Nachrichtendienste geltenden Rechtsrahmen zu klären, sowie Prüfung der Möglichkeiten, ausschließlich Cloud-Server zu nutzen, die sich auf EU-Hoheitsgebiet befinden;

- ein Plan für die Verwendung von mehr Verschlüsselungstechnologien, insbesondere die durchgängige authentifizierte Verschlüsselung für alle IT- und Kommunikationsdienste, wie Cloud-Computing, E-Mail, Sofortnachrichten und Telefonie;

- die Verwendung elektronischen Signaturen in E-Mails;

- ein Plan für die Verwendung eines vorgegebenen Verschlüsselungsstandards wie GNU Privacy Guard für E-Mails, mit dem gleichzeitig die Verwendung digitaler Signaturen möglich wäre;

- die Möglichkeit für die Einrichtung eines sicheren Dienstes für Sofortnachrichten im Parlament, der für eine sichere Kommunikation sorgt, wobei sich auf dem Server nur verschlüsselte Inhalte befinden;

102. fordert alle Gemeinschaftsorgane und EU-Einrichtungen, insbesondere den Europäischen Rat, den Rat, den Europäischen Auswärtigen Dienst (einschließlich der EU-Delegationen), die Kommission, den Gerichtshof und die Europäische Zentralbank, auf, in Zusammenarbeit mit ENISA, Europol und den CERT-Teams bis spätestens Dezember 2014 ähnliche Maßnahmen zu ergreifen; fordert die Mitgliedstaaten auf, ähnliche Bewertungen durchzuführen;

103. betont, dass in Bezug auf das außenpolitische Vorgehen der EU Bewertungen des damit zusammenhängenden Haushaltsbedarfs durchgeführt und beim Europäischen Auswärtigen Dienst (EAD) unverzüglich erste Maßnahmen ergriffen und in angemessenem Umfang Mittel im Entwurf des Haushalts für das Jahr 2015

zugewiesen werden müssen;

104. ist der Ansicht, dass die IT-Großsysteme im Raum der Freiheit, der Sicherheit und des Rechts, wie das Schengener Informationssystem der zweiten Generation, das Visa-Informationssystem, Eurodac und mögliche zukünftige Systeme wie das System der EU zur elektronischen Erteilung von Reisebewilligungen (ESTA) auf eine Weise entwickelt und betrieben werden sollten, durch die sichergestellt wird, dass die Datensicherheit nicht durch Anfragen vonseiten der Behörden von Drittländern gefährdet wird; fordert eu-LISA auf, dem Parlament bis Ende 2014 Bericht über die Zuverlässigkeit der bestehenden Systeme zu erstatten;

105. fordert die Kommission und den EAD auf, Maßnahmen auf internationaler Ebene, insbesondere bei den VN, und in Zusammenarbeit mit interessierten Partnern zu ergreifen, um eine EU-Strategie für die demokratische Verwaltung des Internets umzusetzen und eine unzulässige Beeinflussung der Tätigkeiten von ICANN und IANA durch einzelne Einrichtungen, Unternehmen oder Staaten zu verhindern, indem für eine angemessene Vertretung aller interessierten Parteien in diesen Einrichtungen gesorgt, zugleich jedoch eine Erleichterung der staatlichen Kontrolle oder Zensur bzw. die „Balkanisierung“ und Zersplitterung des Internets vermieden wird;

106. fordert, dass die EU bei der Gestaltung der Architektur und der Verwaltung des Internets die Initiative ergreift, um die Risiken im Zusammenhang mit Datenflüssen und Datensicherung anzugehen und mehr Datensparsamkeit und Transparenz und weniger die zentrale Massenspeicherung von Rohdaten sowie die Verlegung des Internetverkehrs oder die vollständige Ende-zu-Ende-Verschlüsselung des gesamten Internetverkehrs anzustreben, um die aktuellen Risiken zu vermeiden, die mit der unnötigen Verlegung von Datenverkehr auf Hoheitsgebiete von Ländern einhergehen, welche die grundlegenden Standards in Bezug auf Grundrechte, Datenschutz und Privatsphäre nicht einhalten;

107. setzt sich dafür ein, Folgendes zu fördern:

- Suchmaschinen und soziale Netze der EU als sachdienlicher Schritt in Richtung auf die IT-Unabhängigkeit für die EU;

- europäische IT-Dienstleister;

- die generelle Verschlüsselung der Kommunikation einschließlich der E-Mail- und SMS-Kommunikation;

- vorrangige Elemente der europäischen Informationstechnologie, wie zum Beispiel Lösungen für Client-Server-Betriebssysteme, die Nutzung von quelloffenen Standards, die Entwicklung europäischer Bauteile für die Netzkopplung, z. B. Router;

108. fordert die Mitgliedstaaten auf, in Zusammenarbeit mit ENISA, dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität von Europol, den CERT-Teams, den nationalen Datenschutzbehörden und den Dienststellen zur Bekämpfung der Cyberkriminalität eine Sicherheitskultur zu entwickeln und eine Informations- und Sensibilisierungskampagne anzustoßen, um die Bürgerinnen und Bürger in die Lage

zu versetzen, fundiertere Entscheidungen darüber zutreffen, welche persönlichen Daten sie online stellen und wie sie diese besser schützen können, auch mithilfe von Verschlüsselung und sicherem Cloud-Computing, wobei die in der Universaldienstrichtlinie vorgesehenen Plattformen für Informationen von allgemeinem Interesse umfassend genutzt werden;

109. fordert die Kommission auf, bis Dezember 2014 Gesetzesvorschläge zu unterbreiten, um die Software- und Hardwarehersteller zu mehr Sicherheit und Datenschutz mittels Standardfunktionen in ihren Produkten anzuhalten, unter anderem einschließlich durch die Einführung negativer Anreize für die unzulässige und unverhältnismäßige Massensammlung von personenbezogenen Daten und einer gesetzlichen Haftung seitens der Hersteller für nicht behobene, bekannte Schwachstellen, fehlerhafte oder unsichere Produkte oder die Installation von geheimen „Backdoors“ („Hintertüren“), die einen unerlaubten Zugang zu und die Verarbeitung von Daten ermöglichen; fordert die Kommission in diesem Zusammenhang auf, die Möglichkeit der Einrichtung eines Zertifizierungs- oder Validierungssystems für IT-Hardware einschließlich Prüfverfahren auf EU-Ebene abzuschätzen, das die Integrität und Sicherheit der Produkte sicherstellen soll;

Wiederherstellung des Vertrauens

110. ist überzeugt, dass die Untersuchung, abgesehen von der Notwendigkeit einer Änderung der Rechtsvorschriften, gezeigt hat, dass die USA das Vertrauen ihrer EU-Partner wiedererlangen müssen, da es in erster Linie um die Aktivitäten der US-Geheimdienste geht;

111. weist darauf hin, dass die Vertrauenskrise sich auf folgende Bereiche ausgedehnt hat:

– den Geist der Zusammenarbeit innerhalb der EU, da die Aktivitäten einiger nationaler Geheimdienste das Erreichen der Ziele der Union gefährden können;

– die Bürgerinnen und Bürger, die begreifen, dass nicht nur Drittstaaten oder multinationale Unternehmen, sondern auch die eigenen Regierungen sie ausspähen könnten;

– die Achtung der Grundrechte, der Demokratie und der Rechtsstaatlichkeit sowie die Glaubwürdigkeit der demokratischen, rechtlichen und parlamentarischen Garantien und Aufsicht in einer digitalen Gesellschaft;

Zwischen der EU und den USA

112. verweist auf die wichtige historische und strategische Partnerschaft zwischen den Mitgliedstaaten der EU und den USA, auf der Grundlage eines gemeinsamen Glaubens an Demokratie, Rechtsstaatlichkeit und Grundrechte;

113. ist der Überzeugung, dass die Massenüberwachung von Bürgerinnen und Bürgern und die Ausspähung von führenden Politikern durch die USA die Beziehungen zwischen der EU und den USA ernsthaft beschädigt und sich negativ auf das Vertrauen in US-Organisationen ausgewirkt haben, die in der EU tätig sind; dies wird durch das Fehlen

gerichtlicher und verwaltungstechnischer Rechtsmittel für Entschädigungen für EU-Bürgerinnen und Bürger gemäß den US-Gesetzen noch verschlimmert, insbesondere bei Überwachungsaktivitäten für Geheimdienstzwecke;

114. erkennt an, dass die transatlantische Partnerschaft angesichts der globalen Herausforderungen, vor denen die EU und die USA stehen, weiter gestärkt werden muss und dass es von zentraler Bedeutung ist, dass die transatlantische Zusammenarbeit bei der Bekämpfung des Terrorismus auf einer neuen Vertrauensbasis fortgesetzt wird, die auf der wirklichen gemeinsamen Achtung der Rechtsstaatlichkeit und der Ablehnung aller willkürlichen Praktiken der Massenüberwachung beruht; fordert daher mit Nachdruck, dass von den USA klare Maßnahmen ergriffen werden, um das Vertrauen wiederherzustellen, und dass die gemeinsamen, der Partnerschaft zugrundeliegenden Werte wieder stärker betont werden müssen;

115. ist zu einer aktiven Beteiligung an einem Dialog mit den Amtskollegen in den USA bereit, damit in der laufenden Debatte in der Öffentlichkeit und im Kongress der USA über Reformen in Bezug auf die Überwachung und die Überprüfung der Geheimdienstaufsicht das Recht von EU-Bürgerinnen und -Bürgern, Einwohnern oder anderer durch EU-Recht geschützten Personen auf Privatsphäre und andere Rechte angesprochen wird, die gleichen Rechte auf Auskunft und Schutz der Privatsphäre in den US-Gerichten, einschließlich Rechtsmittel, garantiert werden, beispielsweise durch eine Änderung des „Privacy Act“ und des Electronic Communications Privacy Act und durch Ratifizierung des ersten Fakultativprotokolls zum Internationalen Pakt der Vereinten Nationen über bürgerliche und politische Rechte (IPBPR), so dass die derzeitige Diskriminierung nicht immer fortgesetzt wird;

116. fordert mit Nachdruck, dass notwendige Reformen durchgeführt und den Europäern wirksame Garantien gegeben werden, um sicherzustellen, dass die Nutzung von Überwachung und Datenverarbeitung für die Zwecke ausländischer Geheimdienste verhältnismäßig, durch eindeutig festgelegte Bedingungen beschränkt ist und mit einem begründeten Verdacht und einem hinreichendem Verdacht auf terroristische Aktivitäten zusammenhängt; betont, dass diese Zwecke einer transparenten gerichtlichen Kontrolle unterliegen müssen;

117. ist der Auffassung, dass eindeutige politische Signale von unseren amerikanischen Partnern notwendig sind, die zeigen, dass die USA zwischen Verbündeten und Gegnern unterscheiden können;

118. fordert die Kommission und die US-Regierung auf, im Rahmen der laufenden Verhandlungen über ein Rahmenabkommen zwischen der EU und den USA über die Datenübertragung für Zwecke der Strafverfolgung das Recht von EU-Bürgerinnen und -Bürgern auf Auskunft und Rechtsbehelf anzusprechen und diese Verhandlungen vor dem Sommer 2014 entsprechend der beim Treffen der Justiz- und Innenminister der EU und der USA am 18. November 2013 eingegangenen Verpflichtung abzuschließen;

119. empfiehlt den USA, dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarats beizutreten, so

wie sie im Jahr 2001 das Übereinkommen über Computerkriminalität unterzeichnet haben, und auf diese Weise die gemeinsame Rechtsgrundlage zwischen den transatlantischen Verbündeten zu stärken;

120. fordert die EU-Organe auf, Möglichkeiten zu erkunden, einen Verhaltenskodex mit den USA zu vereinbaren, mit dem sichergestellt würde, dass EU-Organe und -einrichtungen nicht vonseiten der USA ausgespäht werden;

Innerhalb der Europäischen Union

121. ist zudem der Ansicht, dass die Beteiligung und Aktivitäten von Mitgliedstaaten der EU zu einem Vertrauensverlust, auch zwischen Mitgliedstaaten und zwischen EU-Bürgern und den Behörden ihrer Mitgliedstaaten, geführt haben; ist der Auffassung, dass nur die volle Klarheit über die Zwecke und Mittel der Überwachung, eine öffentliche Debatte und schließlich eine Überarbeitung der Rechtsvorschriften, einschließlich einer Beendigung der Massenüberwachungsmaßnahmen und der Stärkung der gerichtlichen und parlamentarischen Kontrolle, es ermöglichen werden, das verlorene Vertrauen wiederherzustellen; weist erneut auf die Schwierigkeiten hin, die mit der Entwicklung einer umfassenden EU-Sicherheitspolitik verbunden sind, wenn solche Massenüberwachungsmaßnahmen aktuell sind, und betont, dass der EU-Grundsatz der loyalen Zusammenarbeit erfordert, dass die Mitgliedstaaten Abstand davon nehmen, Geheimdiensttätigkeiten auf dem Hoheitsgebiet anderer Mitgliedstaaten durchzuführen;

122. stellt fest, dass einige Mitgliedstaaten eine bilaterale Kommunikation mit den US-Behörden über Spionagevorwürfe anstrengen und dass einige von ihnen sogenannte „Anti-Spionage-Abkommen“ abgeschlossen haben (Vereinigtes Königreich) oder einen solchen Abschluss planen (Deutschland, Frankreich); betont, dass diese Mitgliedstaaten den Interessen der EU und dem Rechtsrahmen der EU als Ganzes gerecht werden müssen; erachtet solche bilateralen Abkommen für kontraproduktiv und irrelevant, da es für dieses Problem einer europäischen Lösung bedarf; fordert den Rat auf, das Parlament über die Entwicklungen der Mitgliedstaaten über ein EU-weites gegenseitiges Anti-Spionage-Abkommen zu informieren;

123. ist der Ansicht, dass solche Abkommen nicht gegen die Verträge der Union, insbesondere nicht gegen den Grundsatz der loyalen Zusammenarbeit (gemäß Artikel 4 Absatz 3 EUV) verstoßen oder EU-Strategien im Allgemeinen, und den Binnenmarkt, den lauteren Wettbewerb und die wirtschaftliche, industrielle und soziale Entwicklung im Besonderen, untergraben dürfen; beschließt, solche Abkommen in jedem Fall auf ihre Vereinbarkeit mit europäischem Recht zu prüfen, und behält sich das Recht vor, Verfahren einzuleiten, wenn sich erweisen sollte, dass solche Abkommen zum Zusammenhalt der Union oder den wesentlichen Grundsätzen, auf denen sie beruht, im Widerspruch stehen;

124. fordert die Mitgliedstaaten dazu auf, Anstrengungen zu unternehmen, um für eine bessere Kooperation mit Blick auf die Spionageabwehr in Zusammenarbeit mit den einschlägigen EU-Organen und Agenturen zum Schutz der EU-Bürger und Institutionen, der europäischen Unternehmen, der EU-Industrie und der IT-Infrastrukturen und -Netze sowie der europäischen Forschung zu sorgen; hält die

aktive Einbeziehung von Interessenvertretern der EU für eine Vorbedingung für einen wirksamen Informationsaustausch; weist darauf hin, dass Bedrohungen der Sicherheit internationaler, diffuser und komplexer geworden sind und daher eine verstärkte europäische Zusammenarbeit erfordern; ist der Auffassung, dass sich diese Entwicklung besser in den Verträgen widerspiegeln sollte, und fordert daher eine Überarbeitung der Verträge, um den Begriff der loyalen Zusammenarbeit zwischen den Mitgliedstaaten und der Union, was das Ziel der Schaffung eines Raumes der Sicherheit anbelangt, zu stärken und um gegenseitiges Ausspionieren zwischen den Mitgliedstaaten in der Union zu verhindern;

125. erachtet abhörsichere Kommunikationsstrukturen (E-Mail und Telekommunikation, einschließlich Festnetz- und Mobiltelefonen) und abhörsichere Sitzungsräume in allen wichtigen EU-Institutionen und EU-Delegationen für absolut notwendig; fordert daher die Einrichtung eines verschlüsselten EU-internen E-Mail-Systems;

126. fordert den Rat und die Kommission auf, dem am 23. Mai vom Europäischen Parlament angenommenen Vorschlag für eine Verordnung des Europäischen Parlaments über Einzelheiten der Ausübung des Untersuchungsrechts des Europäischen Parlaments und zur Aufhebung des Beschlusses 95/167/EG, Euratom, EGKS des Europäischen Parlaments, des Rates und der Kommission, der auf der Grundlage von Artikel 226 AEUV vorgelegt wurde, unverzüglich zuzustimmen; fordert eine Überarbeitung des Vertrags, um solche Untersuchungsbefugnisse auszuweiten, um alle Zuständigkeits- oder Aktivitätsbereiche der Union ohne Einschränkungen und Ausnahmen abzudecken und die Möglichkeit der eidesstattlichen Befragung einzuschließen;

International

127. fordert die Kommission auf, spätestens im Januar 2015 eine EU-Strategie für eine demokratische Verwaltung des Internets vorzulegen;

128. fordert die Mitgliedstaaten auf, dem Appell der 35. Internationalen Konferenz der Datenschutzbeauftragten zu folgen und sich für die Annahme eines Zusatzprotokolls zu Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte (IPBPR) einzusetzen, das auf den von der Internationalen Konferenz entwickelten und bestätigten Standards und den Bestimmungen der Allgemeinen Bemerkung Nr. 16 des UN-Menschenrechtsausschusses zum Pakt beruhen sollte, um weltweit geltende Standards für den Datenschutz und den Schutz der Privatsphäre im Einklang mit dem Rechtsstaatsprinzip zu schaffen; fordert die Mitgliedstaaten auf, in diesem Zusammenhang eine internationale UN-Agentur zu fordern, die insbesondere für die Beobachtung des Aufkommens von Überwachungsinstrumenten und für die Regulierung und Prüfung ihrer Einsatzzwecke zuständig ist; fordert die Hohe Vertreterin/Vizepräsidentin der Kommission und den Europäischen Auswärtigen Dienst auf, im Vorfeld tätig zu werden;

129. fordert die Mitgliedstaaten auf, eine kohärente und belastbare Strategie im Rahmen der Vereinten Nationen zu entwickeln, mit der insbesondere die von Brasilien und Deutschland initiierte Resolution „Das Recht auf Privatsphäre im digitalen Zeitalter“ unterstützt wird, die vom Dritten Ausschuss der Generalversammlung der Vereinten

Nationen (Menschenrechtsausschuss) am 27. November 2013 verabschiedet wurde, sowie weitere Maßnahmen zum Schutz des Grundrechts auf Privatsphäre und Datenschutz auf internationaler Ebene zu ergreifen, zugleich jedoch eine Erleichterung der staatlichen Kontrolle oder Zensur bzw. die Zersplitterung des Internets zu vermeiden, einschließlich einer Initiative für einen internationalen Vertrag, durch den solche Massenüberwachungsmaßnahmen verboten werden und eine Aufsichtsbehörde eingerichtet wird;

Vorrangiges Programm: Ein europäischer digitaler Habeas-Corpus-Grundsatz - Schutz der Grundrechte in einem digitalen Zeitalter

130. beschließt, den Bürgerinnen und Bürgern, Organen und Mitgliedstaaten der EU die vorstehenden Empfehlungen als vorrangiges Programm für die nächste Wahlperiode vorzulegen;

131. beschließt, „Einen europäischen digitalen Habeas-Corpus-Grundsatz - Schutz der Grundrechte in einem digitalen Zeitalter“ mit den folgenden 8 Aktionen einzuführen dessen Umsetzung es überwachen wird:

Aktion 1: Annahme des Datenschutzpakets im Jahr 2014;

Aktion 2: Abschluss des Rahmenabkommens zwischen der EU und den USA zur Gewährleistung des Grundrechts der Bürgerinnen und Bürger auf Schutz der Privatsphäre und Datenschutz, um ordnungsgemäße Rechtsbehelfe für EU-Bürgerinnen und -Bürger auch im Falle von Datenübermittlungen für Strafverfolgungszwecke von der EU in die USA sicherzustellen;

Aktion 3: Aussetzen der Grundsätze der „Safe-Harbour“-Vereinbarung, bis eine umfassende Überprüfung durchgeführt wurde und derzeit bestehende Schlupflöcher geschlossen wurden, um sicherzustellen, dass die Übermittlung von persönlichen Daten von der Union in die USA für kommerzielle Zwecke nur im Einklang mit den höchsten EU-Standards erfolgen kann;

Aktion 4: Aussetzen des TFTP-Abkommens, bis: (i) die Verhandlungen über das Rahmenabkommen abgeschlossen wurden; (ii) eine gründliche Untersuchung auf der Grundlage einer EU-Analyse durchgeführt wurde und alle vom Parlament in seiner Entschließung von 23. Oktober geäußerten Bedenken angemessen ausgeräumt wurden;

Aktion 5: Bewertung jedes Abkommens, Mechanismus oder Austauschs mit Drittländern mit Auswirkungen auf personenbezogene Daten, um sicherzustellen, dass das Recht auf den Schutz der Privatsphäre und auf den Schutz personenbezogener Daten nicht durch Überwachungsmaßnahmen verletzt wird, und Ergreifen der notwendigen Folgemaßnahmen;

Aktion 6: Schutz der Rechtsstaatlichkeit und der Grundrechte der EU-Bürger (einschließlich durch die Bedrohung der Pressefreiheit), des Rechts der Öffentlichkeit auf unparteiische Informationen und des Berufsgeheimnisses (einschließlich der Beziehungen zwischen Anwalt und Mandant) sowie

Gewährleistung eines erweiterten Schutzes für Informanten;

Aktion 7: Entwickeln einer europäischen Strategie für eine größere Unabhängigkeit im IT-Bereich (eines „Digital New Deal“, einschließlich der Bereitstellung angemessener Ressourcen sowohl auf einzelstaatlicher als auch auf EU-Ebene) zur Förderung des Wachstums der IT-Branche, das es europäischen Unternehmen ermöglicht, den Wettbewerbsvorteil der EU bei der Privatsphäre auszunutzen;

Aktion 8: Entwickeln der EU als Maßstab für eine demokratische und neutrale Verwaltung des Internets;

132. fordert die Gemeinschaftsorgane und die Mitgliedstaaten auf, den „Europäischen digitalen Habeas-Corpus-Grundsatz - Schutz der Grundrechte in einem digitalen Zeitalter“ zu unterstützen und zu fördern; verpflichtet sich, als Anwalt der Rechte der EU-Bürgerinnen und -Bürger zu agieren, mit folgendem Zeitplan zur Überwachung der Umsetzung:

- April - Juli 2014: eine Beobachtungsgruppe basierend auf dem LIBE-Untersuchungsteam, zuständig für die Überwachung neuer Enthüllungen in Bezug auf den Untersuchungsauftrag und die Prüfung der Umsetzung dieser Entschließung;

- von Juli 2014 an: ein ständiger Aufsichtsmechanismus für Datenübertragungen und Rechtsbehelfe innerhalb des zuständigen Ausschusses;

- Frühjahr 2014: ein förmlicher Aufruf an den Rat, den „Europäischen digitalen Habeas-Corpus-Grundsatz - Schutz der Grundrechte in einem digitalen Zeitalter“ in die nach Artikel 68 AEUV zu verabschiedenden Richtlinien aufzunehmen;

- Herbst 2014: eine Selbstverpflichtung, dass die nächste Kommission ihre Zustimmung von dem „Europäischen digitalen Habeas-Corpus-Grundsatz - Schutz der Grundrechte in einem digitalen Zeitalter“ und den zugehörigen Empfehlungen als zentralen Kriterien abhängig macht;

- 2014: Konferenz, bei der hochrangige europäische Experten auf den verschiedenen, der IT-Sicherheit dienlichen Gebieten (u. a. Mathematik, Kryptografie und Datenschutztechnologien) zusammengeführt werden, um eine IT-Strategie der EU für die nächste Legislaturperiode zu unterstützen;

- 2014-2015: regelmäßiges Einberufen einer Gruppe für Vertrauen/Daten/Bürgerrechte zwischen dem Europäischen Parlament und dem Kongress der USA, sowie mit den Parlamenten anderer beteiligter Drittländer, darunter das Parlament Brasiliens;

- 2014-2015: Konferenz mit den Geheimdienstaufsichtsgremien der europäischen nationalen Parlamente;

133. beauftragt seinen Präsidenten, diese Entschließung dem Europäischen Rat, dem Rat, der Kommission, den Parlamenten und Regierungen der Mitgliedstaaten, den nationalen Datenschutzbehörden, dem EDSB, eu-LISA, ENISA, der Grundrechteagentur, der Artikel-29-Datenschutzgruppe, dem Europarat, dem Kongress der Vereinigten Staaten von Amerika, der US-Regierung, dem Präsidenten, der Regierung und dem Parlament der Föderativen Republik Brasilien und dem Generalsekretär der Vereinten Nationen zu übermitteln.

BEGRÜNDUNG

„Die Aufgabe des Souveräns, ob Monarch oder Versammlung, ergibt sich aus dem Zweck, zu dem er mit der souveränen Gewalt betraut wurde, nämlich der Sorge für die Sicherheit des Volkes."
Hobbes, Leviathan (Kapitel XXX)

„Wir können unsere Gesellschaft anderen gegenüber nicht preisen, wenn wir von den grundlegenden Normen abrücken, die sie des Preisens würdig macht."
Lord Bingham of Cornhill,
Ehem. Lord Chief Justice of England and Wales

Methodik

Seit Juli 2013 war der LIBE-Untersuchungsausschuss mit der äußerst anspruchsvollen Aufgabe betraut, das Mandat[1] des Plenums zur Untersuchung der elektronischen Massenüberwachung von EU-Bürgern in einem äußerst kurzen Zeitrahmen von weniger als sechs Monaten wahrzunehmen.

In diesem Zeitraum veranstaltete er 15 Anhörungen, die jedes der spezifischen Cluster-Themen erfassten, welche in der Entschließung vom 4. Juli festgelegt worden waren. Er stützte sich dabei auf die Beiträge von Experten gleichermaßen aus der EU wie aus den USA, die ein breites Spektrum an Wissen und Hintergründen einbrachten: EU-Institutionen, einzelstaatliche Parlamente, US-Kongress, Wissenschaftler, Journalisten, die Zivilgesellschaft, Sicherheits- und Technologie-Fachleute sowie Vertreter der Privatwirtschaft. Außerdem hat eine Abordnung des LIBE-Ausschusses vom 28. bis 30. Oktober Washington besucht, um dort mit Vertretern sowohl der Exekutive als auch der Legislative zusammenzutreffen (Wissenschaftlern, Rechtsanwälten, Sicherheitsfachleuten, Wirtschaftsvertretern)[2]. Zeitgleich hielt sich eine Delegation des Ausschusses für auswärtige Angelegenheiten (AFET) in der Stadt auf. Es kam zu einer Reihe gemeinsamer Begegnungen.

Gemeinsam mit dem Berichterstatter, den Schattenberichterstattern[3] aus den verschiedenen Fraktionen sowie drei Mitgliedern des AFET-Ausschusses[4] wurden zur Vorstellung von zentralen Erkenntnissen, die bei der Untersuchung gewonnen worden waren, diverse Arbeitspapiere[5] verfasst. Der Berichterstatter möchte hiermit allen Schattenberichterstattern und AFET-Mitgliedern für ihre enge Zusammenarbeit wie auch ihr über den gesamten Verlauf dieses anspruchsvollen Prozesses an den Tag gelegtes Engagement seinen Dank aussprechen.

---

[1] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_ta-prov(2013)0322_de.pdf
[2] Vgl. Bericht der Washington-Delegation
[3] Liste der Schattenberichterstatter: Axel Voss (PPE), Sophia in't Veld (ALDE), Jan Philipp Albrecht (Verts/ALE), Timothy Kirkhope (EFD), Cornelia Ernst (GUE/NGL).
[4] Liste der AFET-Mitglieder: José Ignacio Salafranca Sánchez-Neyra (PPE), Ana Gomes (S&D), Annemie Neyts-Uyttebroeck (ALDE).
[5] Siehe Anhang I.

Ausmaß des Problems

Eine zunehmende Akzentuierung von Fragen der Sicherheit hat im Zusammenspiel mit technologischen Weiterentwicklungen die Möglichkeit geschaffen, dass Staaten heute mehr als je zuvor über ihre Bürger wissen. Durch ihre Fähigkeit, Daten über den Inhalt von Kommunikation sowie Metadaten zu sammeln und die elektronischen Aktivitäten der Bürger, insbesondere die Benutzung von Smartphones und Tablet-Computern, zu verfolgen, sind die Nachrichtendienste de facto in der Lage, so gut wie alles über eine Person in Erfahrung zu bringen. Dies hat **zu einem grundlegenden Wandel in der Arbeit und den Praktiken der Nachrichtendienste beigetragen, weg vom traditionellen Konzept der gezielten Überwachung als angemessene und verhältnismäßige Maßnahme zur Terrorismusbekämpfung, hin zu einem System der Massenüberwachung.**

Dieser Prozess der zunehmenden Massenüberwachung war nicht Gegenstand einer öffentlichen Debatte oder einer demokratischen Entscheidungsfindung. Es bedarf einer Diskussion über den Zweck und das Ausmaß der Überwachung und ihren Platz in einer demokratischen Gesellschaft. Ist die durch Edward Snowdens Enthüllungen geschaffene Situation ein Anzeichen für eine allgemeine gesellschaftliche Hinwendung zu einer Einstellung, wonach für mehr Sicherheit das Ende der Privatsphäre in Kauf genommen wird? Sehen wir uns einer Verletzung der Privatsphäre und Intimität in einem solchen Ausmaß gegenüber, dass nicht nur Kriminelle, sondern auch IT-Konzerne und Nachrichtendienste in der Lage sind, das Leben der Bürger in allen Einzelheiten zu durchleuchten**?** Handelt es sich hierbei um eine Gegebenheit, die ohne weitere Diskussion einfach hinzunehmen ist? Oder ist es Sache des Gesetzgebers, die Politik und die vorliegenden juristischen Mittel zur Begrenzung der Gefahren und zur Abwendung von weiterem Schaden für den Fall anzupassen, dass einmal weniger demokratisch gesinnte Kräfte an die Macht gelangen sollten?

Reaktionen auf Massenüberwachung und eine öffentliche Debatte

Innerhalb der EU wird über Massenüberwachung in uneinheitlicher Weise debattiert. So wird in vielen Mitgliedstaaten kaum öffentlich debattiert, und auch der Umfang der Wahrnehmung des Themas durch die Medien stellt sich unterschiedlich dar. Auf das größte Echo sind dem Anschein nach die Enthüllungen in Deutschland gestoßen, wo die Diskussionen über deren Folgen unter großer Anteilnahme der Öffentlichkeit geführt werden. Im Vereinigten Königreich und Frankreich sind den von den Tageszeitungen The Guardian und Le Monde unternommenen Untersuchungen zum Trotz die Reaktionen eher begrenzt, was dem Umstand zugeschrieben wird, dass deren nationale Nachrichtendienste in gemeinsame Aktivitäten mit der NSA verstrickt sein sollen. Bei seiner Untersuchung hatte der LIBE-Ausschuss Gelegenheit, wertvolle Beiträge von Seiten der parlamentarischen Aufsichtsgremien Belgiens, der Niederlande, Dänemarks und sogar Norwegens anzuhören; das britische und das französische Parlament hingegen haben eine Mitarbeit abgelehnt. Diese Unterschiede veranschaulichen einmal mehr das unterschiedliche Maß an Kontroll- und Überwachungsmöglichkeiten, die innerhalb der EU auf diesem Gebiet bestehen, und unterstreichen, dass es unter den parlamentarischen Aufsichtsgremien einer stärkeren Zusammenarbeit bedarf.

Im Gefolge der durch Edward Snowden in den Massenmedien getätigten Enthüllungen haben

vor allem zwei Formen der Reaktion die öffentliche Debatte geprägt. Auf der einen Seite finden sich jene, die den veröffentlichten Informationen die Legitimität mit der Begründung absprechen, dass die meisten Berichte in den Medien auf Fehlinterpretationen beruhten. Daneben ziehen viele die Stichhaltigkeit der Enthüllungen, ohne diese zu widerlegen, angesichts von Behauptungen in Zweifel, dass von diesen eine Gefährdung der nationalen Sicherheit und der Terrorismusbekämpfung ausgehe.

Auf der anderen Seite stehen jene, nach deren Einschätzung die gelieferten Angaben eine fundierte öffentliche Debatte erfordern angesichts des Ausmaßes der hierdurch aufgeworfenen Probleme im Hinblick auf für eine Demokratie zentrale Fragen wie: Rechtsstaatlichkeit, Grundrechte, Privatsphäre von Bürgern, Rechenschaftspflicht von Strafverfolgungsbehörden und Nachrichtendiensten gegenüber der Öffentlichkeit usw. Zu Letzteren zählen fraglos die Journalisten und Herausgeber der in die Enthüllungen eingeweihten weltgrößten Pressekanäle, darunter The Guardian, Le Monde, Der Spiegel, The Washington Post und Glenn Greenwald.

Die beiden vorstehend beschriebenen, jeweils durch eine ganze Reihe von Beweggründen motivierten Reaktionsweisen führen unter Umständen zu ganz gegensätzlichen Urteilen darüber, wie die EU reagieren oder nicht reagieren sollte.

Fünf Gründe dafür, nicht tätig zu werden

– *Das Argument „Nachrichtendienste/Nationale Sicherheit“: fällt nicht in die Zuständigkeit der EU*

  Die von Edward Snowden getätigten Enthüllungen beziehen sich auf nachrichtendienstliche Tätigkeiten der USA und einiger Mitgliedstaaten, die nationale Sicherheit ist jedoch Sache der Mitgliedstaaten, und die EU verfügt diesbezüglich (außer in Fragen der EU-internen Sicherheit) über keine Zuständigkeit, weshalb auch keine Maßnahmen auf EU-Ebene ergriffen werden können.

– *Das Argument „Terrorismus“: Gefahr durch den Whistleblower*

  Jegliche aufgrund dieser Enthüllungen getroffene oder auch nur erwogene Folgemaßnahme bedeutet eine weitere Schwächung der Sicherheit der USA wie auch der EU, da diese nicht die Veröffentlichung von Dokumenten verurteilt, deren Inhalte, wie beteiligte Medienvertreter erklären, selbst in überarbeiteter Form terroristischen Vereinigungen wertvolle Informationen liefern können.

– *Das Argument „Verrat“: die Illegitimität des Whistleblowers*

  Wie manche vor allem in den USA und im Vereinigten Königreich einwenden, ist jede eingeleitete Debatte oder erwogene Maßnahme im Gefolge der von E. Snowden getätigten Enthüllungen per se parteiisch und irrelevant, da sie auf einem Akt des Verrats gründen würde.

– *Das Argument „Realismus“: allgemeine strategische Interessen*

Selbst im Falle, dass sich einzelne Fehler oder ungesetzliche Handlungen bestätigen sollten, sind diese gegen die Notwendigkeit abzuwägen, die besondere Beziehung zwischen den USA und der EU zur Wahrung der gemeinsamen wirtschaftlichen und geschäftlichen sowie außenpolitischen Interessen fortzuführen.

– *Das Argument „Vertrauenswürdige Regierung“: Legitimität der Regierung*

Die Regierungen der USA und der EU sind demokratisch gewählt. In Sicherheitsfragen werden diese demokratischen Normen grundsätzlich auch dann gerecht, wenn zur Terrorismusbekämpfung nachrichtendienstliche Tätigkeiten unternommen werden. Diese „Vermutung einer verantwortungsbewussten Regierungsführung nach rechtstaatlichen Grundsätzen“ beruht nicht allein auf dem guten Willen der Vollzugskräfte, sondern auch auf den in der jeweiligen Verfassung verankerten Kontroll- und Überwachungsmechanismen.

Wie man sieht, sind die Gründe, nicht aktiv zu werden, zahlreich und gewichtig. Dies mag erklären, warum die Regierungen der meisten Mitgliedstaaten nach anfänglich heftigen Reaktionen es bevorzugt haben, nicht tätig zu werden. Die vom Ministerrat getroffene Hauptmaßnahme bestand in der Einrichtung einer „transatlantischen Gruppe von Datenschutzexperten“, die nach dreimaligem Zusammentreffen einen Abschlussbericht vorgelegt hat. Eine zweite Gruppe soll sich zur Erörterung nachrichtendienstlicher Probleme zwischen Behörden der USA und denen der Mitgliedstaaten getroffen haben; hierzu liegen jedoch keine Informationen vor. Der Europäische Rat hat das Überwachungsproblem in einer bloßen Erklärung seitens der Staats- und Regierungschefs angesprochen[1]; bislang haben nur einige wenige einzelstaatliche Parlamente Untersuchungen eingeleitet.

Fünf Gründe dafür, tätig zu werden

– *Das Argument „Massenüberwachung“: In was für einer Gesellschaft wollen wir leben?*

Seit den ersten Enthüllungen im Juni 2013 wird immer wieder auf George Orwells Roman „1984“ verwiesen. Seit den Attentaten vom 11. September 2001 haben eine Schwerpunktsetzung auf Sicherheitsfragen und eine Verlagerung hin zu zielgerichteter, spezifischer Überwachung den Begriff der Privatsphäre erheblich beschädigt und untergraben. Die Geschichte sowohl Europas als auch der USA führt uns die von einer Massenüberwachung ausgehenden Gefahren und die Stufenfolge hin zu Gesellschaftsformen ohne Privatsphäre vor Augen.

– *Das Argument „Grundrechte“:*

Massenhafte und unterschiedslos unternommene Überwachung gefährdet grundlegende

[1] Schlussfolgerungen des Europäischen Rates vom 24.-25. Oktober 2013, insbesondere: „Die Staats- und Regierungschefs nahmen die Absicht von Frankreich und Deutschland zur Kenntnis, bilaterale Gespräche mit den USA im Bestreben zu suchen, noch vor Ende des Jahres zu einem Abkommen über wechselseitige Beziehungen in diesem Bereich zu gelangen. Sie nahmen zur Kenntnis, dass andere EU-Länder eingeladen sind, sich dieser Initiative anzuschließen. Sie verwiesen ferner auf die zwischen der EU und den USA bestehende Arbeitsgruppe zum sachverwandten Thema des Datenschutzes und verlangten diesbezüglich rasche und konstruktive Fortschritte.“

Bürgerrechte wie u. a. das Recht auf Privatsphäre, Datenschutz, Pressefreiheit und den Anspruch auf ein faires Gerichtsverfahren, die ausnahmslos in den EU-Verträgen, der Grundrechtecharta und der EMRK verankert sind. Diese Rechte lassen sich lediglich in dem Umfang umgehen oder im Gegenzug für irgendeinen als Ausgleich erwarteten Nutzen einschränken, den ordnungsgemäß verabschiedete, im Einklang mit den vorgenannten Verträgen stehende Rechtsakte vorsehen.

– Das Argument *„Innere Sicherheit der EU“*

Die einzelstaatliche Zuständigkeit in Bezug auf Nachrichtendienste und Fragen der nationalen Sicherheit schließt eine parallele EU-Zuständigkeit nicht aus. Die ihr durch die EU-Verträge übertragenen Kompetenzen in Fragen der inneren Sicherheit übt die EU in Form von Entscheidungen über eine Anzahl an Rechtsetzungsakten und internationalen Abkommen aus, die auf die Bekämpfung von Schwerkriminalität und Terrorismus abzielen, sowie die Einrichtung einer Strategie der inneren Sicherheit und von Behörden, die in diesem Bereich tätig sind. Daneben sind weitere Dienste entwickelt worden, welche den Bedarf nach einer verstärkten Zusammenarbeit in nachrichtendienstlichen Fragen auf EU-Ebene widerspiegeln: das (beim EAD angesiedelte) EU INTCEN und den (beim Generalsekretariat des Rates angesiedelten) Koordinator für die Terrorismusbekämpfung, beide ohne rechtliche Grundlage.

– *Das Argument „Unzulängliche Aufsicht“*

Auch wenn die Nachrichtendienste eine unverzichtbare Rolle beim Schutz gegen innere und äußere Bedrohungen spielen, müssen sie innerhalb der Grenzen der Gesetze agieren und hierzu einem strikten und gründlichen Aufsichtsmechanismus unterworfen sein. Die demokratische Aufsicht über nachrichtendienstliche Tätigkeiten erfolgt auf einzelstaatlicher Ebene; aufgrund des internationalen Charakters der Sicherheitsbedrohungen indes findet inzwischen ein enormer Informationsaustausch zwischen Mitgliedstaaten und mit Drittländern wie den USA statt. Es bedarf Verbesserungen bei den Aufsichtsmechanismen sowohl auf einzelstaatlicher als auch auf EU-Ebene, damit die üblichen Aufsichtsmechanismen nicht unwirksam werden oder veralten.

– *Die „Abschreckwirkung auf die Medien“ und der Schutz von Whistleblowern*

Die Enthüllungen durch Edward Snowden und die sich daran anschließenden Medienberichte haben die Schlüsselrolle in den Blickpunkt gerückt, die Medien in einer Demokratie dabei zukommt, die Rechenschaftspflicht von Regierungen sicherzustellen. Wenn sich durch Kontrollmechanismen Massenüberwachung nicht verhindern oder beseitigen lässt, ist die Rolle der Medien und der Whistleblower bei der Enthüllung von illegalem Verhalten oder Machtmissbrauch extrem wichtig. Reaktionen seitens US-amerikanischer und britischer Behörden auf die Medien haben die Verwundbarkeit gleichermaßen der Presse wie der Whistleblower und den dringenden Bedarf vor Augen geführt, mehr für deren Schutz zu unternehmen.

Die Europäische Union wird aufgefordert, zwischen einer Politik des „Alles wie gehabt“ (hinreichende Gründe, nicht tätig zu werden und einfach abzuwarten) und einer Politik des „Augenöffnens“ (Überwachung hat es schon früher gegeben, es liegen jedoch genügend

Hinweise für ein nie dagewesenes Ausmaß sowohl hinsichtlich des Umfangs als auch der Möglichkeiten der Nachrichtendienste vor, welches ein Einschreiten der EU erforderlich macht) zu wählen.

Persönliche Freiheit in einer Überwachungsgesellschaft

Im Jahr 1679 vollzog das britische Parlament in Zeiten rivalisierender Rechtsprechungen und zueinander im Widerspruch stehender Gesetze mit der Verabschiedung des *Habeas Corpus Act* einen bedeutenden Schritt zur Sicherstellung des Rechts auf eine richterliche Anhörung. Heutzutage garantieren unsere Demokratien Verurteilten oder Inhaftierten, gegen die in Person ein Strafverfahren eingeleitet worden ist oder die der Rechtsprechung überantwortet werden, angemessene Rechte. Die Daten hingegen, die in digitalen Netzwerken mitgeteilt, verarbeitet, gespeichert und verfolgt werden, bilden einen „Corpus persönlicher Daten“, eine Art digitalen Körper, der jeder Person individuell zu eigen ist und die Möglichkeit schafft, viel über deren Identität, Gewohnheiten und Vorlieben aller Art in Erfahrung zu bringen.

Habeas Corpus ist als fundamentales Rechtsinstrument zur Wahrung der individuellen Freiheit vor staatlicher Willkür anerkannt. Was wir heute benötigen, ist eine Erweiterung dieser Sicherung der persönlichen Freiheit auf das digitale Zeitalter. Das Recht auf Privatsphäre, die Achtung der Integrität und der Würde des Einzelnen stehen auf dem Spiel. Die Massenerfassung von Daten unter Missachtung der EU-Bestimmungen zum Datenschutz und spezifische Verletzungen des Grundsatzes der Verhältnismäßigkeit beim Datenmanagement laufen den konstitutionellen Traditionen der Mitgliedstaaten und den Fundamenten der konstitutionellen Ordnung Europas zuwider.

Die größte Neuerung der Gegenwart besteht darin, dass diese Gefahren sich nicht allein aus kriminellen Handlungen (gegen die der EU-Gesetzgeber eine Reihe von Instrumenten verabschiedet hat) oder möglichen Cyberangriffen durch Behörden von Ländern mit niedrigerem Demokratiestandard ergeben. Immer mehr wird man sich bewusst, dass solche Gefahren auch von Strafverfolgungsbehörden und Nachrichtendiensten demokratischer Staaten ausgehen können, was Bürger oder auch Unternehmen der EU mit Gesetzen in Konflikt geraten lässt, was eine verminderte Rechtssicherheit zur Folge hat angesichts möglicher Verletzungen ihrer Rechte, ohne dass ihnen dabei angemessene Rechtsbehelfe zur Verfügung stünden.

Zur Gewährleistung der Sicherheit personenbezogener Daten bedarf es einer Netz-Governance. Vor dem Entstehen des modernen Staatswesens war die Sicherheit auf inner- wie außerörtlichen Straßen nicht gewährleistet, und die körperliche Unversehrtheit war gefährdet. Heutzutage sind es die Datenautobahnen, denen es, obwohl sie längst unseren Alltag beherrschen, an Sicherheit mangelt. Es gilt, die Integrität digitaler Daten sicherzustellen, einerseits natürlich gegenüber Bedrohungen durch Kriminalität, andererseits jedoch auch gegenüber einem möglichen Missbrauch durch Behörden, Vertragspartner oder auch Privatunternehmen, die mit geheimen richterlichen Ermächtigungen agieren.

Empfehlungen aufgrund der vom LIBE-Ausschuss durchgeführten Untersuchung

Viele der sich heutzutage stellenden Probleme weisen eine große Ähnlichkeit mit denjenigen auf, welche im Rahmen der Untersuchung des Europäischen Parlaments zum Echelon-Programm 2001 aufgezeigt worden waren. Aus dem Umstand, dass es in der

vorangegangenen Legislaturperiode nicht gelungen ist, den Erkenntnissen und Empfehlungen der Echelon-Untersuchung Taten folgen zu lassen, sollten bei dieser Untersuchung wichtige Lehren gezogen werden. Aus eben diesem Grund ist die vorliegende Entschließung, die sowohl die Tragweite der damit in Zusammenhang stehenden Enthüllungen als auch deren fortwährenden Charakter würdigt, vorausschauender Natur, indem sie dafür sorgt, dass spezifische Vorschläge für nachfassende, während der nächsten Wahlperiode des Parlaments zu ergreifende Maßnahmen auf dem Tisch liegen, und auf diese Weise die Erkenntnisse auf der politischen Agenda der EU weiterhin einen prominenten Platz einnehmen.

Auf Grundlage dieser Beurteilung möchte der Berichterstatter dem Parlament hiermit die folgenden Maßnahmen zur Abstimmung vorlegen:

„Ein europäischer digitaler Habeas-Corpus-Grundsatz - Schutz der Grundrechte in einem digitalen Zeitalter“ auf der Grundlage von 8 Aktionen:

Aktion 1: Verabschiedung des Pakets zum Datenschutz im Jahr 2014;

Aktion 2: Abschluss des Rahmenabkommens zwischen der EU und den USA zur Gewährleistung des Grundrechts der Bürger auf Schutz der Privatsphäre und Datenschutz, um ordnungsgemäße Rechtsbehelfs für EU-Bürgerinnen und -Bürger auch im Falle von Datenübermittlungen für Strafverfolgungszwecke von der EU in die USA sicherzustellen;

Aktion 3: Aussetzen der Grundsätze der „Safe-Harbour“-Vereinbarung, bis eine umfassende Überprüfung durchgeführt wurde und derzeit bestehende Schlupflöcher geschlossen wurden, um sicherzustellen, dass die Übermittlung von persönlichen Daten von der Union in die USA für kommerzielle Zwecke nur im Einklang mit den höchsten EU-Standards erfolgen kann;

Aktion 4: Aussetzen des Abkommens über das Programm zum Aufspüren der Finanzierung des Terrorismus bis (i) die Verhandlungen über das Rahmenabkommen abgeschlossen wurden; (ii) eine gründliche Untersuchung auf der Grundlage einer EU-Analyse durchgeführt wurde und alle vom Parlament in seiner Entschließung von 23. Oktober geäußerten Bedenken angemessen ausgeräumt wurden;

Aktion 5: Bewertung jedes Abkommens, Mechanismus oder Austauschs mit Drittländern mit Auswirkungen auf personenbezogene Daten, um sicherzustellen, dass das Recht auf den Schutz der Privatsphäre und auf den Schutz personenbezogener Daten nicht durch Überwachungsmaßnahmen verletzt wird, und Ergreifen der notwendigen Folgemaßnahmen;

Aktion 6: Schutz der Rechtsstaatlichkeit und der Grundrechte der EU-Bürger (einschließlich durch die Bedrohung der Pressefreiheit), des Rechts der Öffentlichkeit auf unparteiische Informationen und des Berufsgeheimnisses (einschließlich der Beziehungen zwischen Anwalt und Mandant) sowie ein erweiterter Schutz für Informanten;

Aktion 7: Entwickeln einer europäischen Strategie für eine größere Unabhängigkeit im IT-Bereich (eines „Digital New Deal“, einschließlich der Bereitstellung

angemessener Ressourcen sowohl auf einzelstaatlicher als auch auf EU-Ebene) zur Förderung des Wachstums der IT-Branche, das es europäischen Unternehmen ermöglicht, den Wettbewerbsvorteil der EU bei der Privatsphäre auszunutzen;

Aktion 8: Entwicklung der EU als Maßstab für eine demokratische und neutrale Verwaltung des Internets.

Nach Abschluss der Untersuchung sollte das Europäische Parlament weiterhin als Anwalt der Rechte der EU-Bürger agieren und die Umsetzungen dabei nach dem folgenden Zeitplan verfolgen:

- April - Juli 2014: eine Beobachtungsgruppe basierend auf dem LIBE-Untersuchungsteam, zuständig für die Überwachung neuer Enthüllungen in Bezug auf den Untersuchungsauftrag und die Prüfung der Umsetzung dieser Entschließung;

- von Juli 2014 an: ein ständiger Aufsichtsmechanismus für Datenübertragungen und Rechtsbehelfe innerhalb des zuständigen Ausschusses;

- Frühjahr 2014: ein förmlicher Aufruf an den Rat, den „Europäischen Digitalen Habeas-Corpus-Grundsatz - Schutz der Grundrechte in einem digitalen Zeitalter“ in die nach Artikel 68 AEUV zu verabschiedenden Richtlinien aufzunehmen;

- Herbst 2014: eine Selbstverpflichtung, dass die nächste Kommission ihre Zustimmung von dem „Europäischen Digitalen Habeas-Corpus-Grundsatz - Schutz der Grundrechte in einem digitalen Zeitalter“ und den zugehörigen Empfehlungen als zentralen Kriterien abhängig macht;

- 2014: Konferenz, bei der hochrangige europäische Experten auf den verschiedenen, der IT-Sicherheit dienlichen Gebieten (u. a. Mathematik, Kryptografie und Datenschutztechnologien) zusammengeführt werden, um eine IT-Strategie der EU für die nächste Wahlperiode zu unterstützen;

- 2014-2015: regelmäßiges Einberufen einer Gruppe für Vertrauen/Daten/Bürgerrechte zwischen dem Europäischen Parlament und dem Kongress der USA, sowie mit den Parlamenten anderer beteiligter Drittländer, einschließlich Brasiliens;

- 2014-2015: Konferenz mit den Geheimdienstaufsichtsgremien der europäischen nationalen Parlamente;

ANHANG I: LISTE DER ARBEITSDOKUMENTE

LIBE-Untersuchungsausschuss

Berichterstatter & Schattenbericht-erstatter als Mitverfasser	Themen	Entschließung des Europäischen Parlaments vom 4. Juli 2013 (siehe Ziffern 15-16)
Claude Moraes (S&D)	Überwachungsprogramme der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger	16 a) b) c) d)
Axel Voss (PPE)	**US-Überwachung von EU-Daten und mögliche Auswirkungen auf transatlantische Abkommen und Zusammenarbeit**	16 a) b) c)
Sophia In't Veld (ALDE) & Cornelia Ernst (GUE)	Demokratische Kontrolle von Nachrichtendiensten der Mitgliedstaaten und Nachrichtendiensten der EU	15, 16 a) c) e)
Jan Philipp Albrecht (Verts/ALE)	Verhältnis zwischen der Überwachungstätigkeit in der EU sowie in den USA und den Datenschutzbestimmungen der Europäischen Union	16 c) e) f)
Timothy Kirkhope (ECR)	„Scope of International, European and national security in the EU perspective"[1] (Ausmaß der internationalen, europäischen und nationalen Sicherheit aus der EU-Perspektive)	16 a) b)
AFET 3 Mitglieder	„Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens" (Außenpolitische Aspekte der Untersuchung zur elektronischen Massenüberwachung von EU-Bürgern)	16 a) b) f)

[1] nicht verteilt.

ANHANG II: LISTE DER ANHÖRUNGEN UND SACHVERSTÄNDIGEN

LIBE-UNTERSUCHUNGSAUSSCHUSS
ZUM ÜBERWACHUNGSPROGRAMM DER NSA,
ÜBERWACHUNGSEINRICHTUNGEN IN MEHREREN MITGLIEDSTAATEN
UND AUSWIRKUNGEN AUF DIE GRUNDRECHTE DER EU-BÜRGER UND DIE
TRANSATLANTISCHE ZUSAMMENARBEIT IM BEREICH JUSTIZ UND INNERES

Im Anschluss an die Entschließung des Europäischen Parlaments vom 4. Juli 2013 (Ziffer 16) hat der LIBE-Ausschuss eine Reihe von Anhörungen abgehalten, um Informationen zu den unterschiedlichen relevanten Aspekten zu sammeln, die Auswirkungen der betreffenden Überwachungstätigkeiten zu bewerten, insbesondere im Hinblick auf die Grundrechte und Datenschutzbestimmungen, die Rechtsdurchsetzungsmechanismen zu untersuchen und Empfehlungen abzugeben, um die Rechte der EU-Bürger zu schützen und die IT-Sicherheit der EU-Institutionen zu stärken.

Datum	Gegenstand	Sachverständige
5. September 2013 15.00 – 18.30 Uhr (Brüssel)	- Aussprache mit den Journalisten, die den Fall aufgedeckt und die Fakten veröffentlicht haben	• Jacques FOLLOROU, Le Monde • Jacob APPELBAUM, investigativer Journalist, Softwareentwickler und Spezialist für Computersicherheit beim Tor-Projekt • Alan RUSBRIDGER, Chefredakteur beim Verlag „Guardian News and Media“ (per Videokonferenz)
	- Nachbereitung der Arbeit des nichtständigen Ausschusses über das Abhörsystem ECHELON	• Carlos COELHO (MdEP), ehemaliger Vorsitzender des nichtständigen Ausschusses über das Abhörsystem ECHELON • Gerhard SCHMID (ehemaliges MdEP und Berichterstatter des ECHELON-Berichts im Jahr 2001) • Duncan CAMPBELL, investigativer Journalist und

		Verfasser des STOA-Berichts „Interception Capabilities 2000“ (Abhörfähigkeiten im Jahr 2000)
12. September 2013 10.00 – 12.00 Uhr (Straßburg)	- Feedback der Sitzung der transatlantischen Expertengruppe EU-USA zum Datenschutz vom 19./20. September 2013 - Arbeitsmethode und Zusammenarbeit mit dem LIBE-Untersuchungsausschuss (unter Ausschluss der Öffentlichkeit) - Aussprache mit der Arbeitsgruppe Datenschutz zu Artikel 29	• Darius ŽILYS, Ratsvorsitz, Direktor der Abteilung für Völkerrecht, litauisches Justizministerium (Ko-Vorsitzender der Ad hoc-Arbeitsgruppe EU-USA zum Datenschutz) • Paul NEMITZ, Direktor GD JUST, Europäische Kommission (Ko-Vorsitzender der Ad hoc-Arbeitsgruppe EU-USA zum Datenschutz) • Reinhard PRIEBE, Direktor GD HOME, Europäische Kommission (Ko-Vorsitzender der Ad hoc-Arbeitsgruppe EU-USA zum Datenschutz) • Jacob KOHNSTAMM, Vorsitzender
24. September 2013 9.00 – 11.30 Uhr und 15.00 – 18.30 Uhr (Brüssel) **Mit AFET**	- Verdacht auf das Ausspionieren durch die NSA von SWIFT-Daten, welche im Programm zum Aufspüren der Finanzierung des Terrorismus verwendet werden - Feedback der Sitzung der transatlantischen Expertengruppe EU-USA zum Datenschutz vom 19./20. September 2013	• Cecilia MALMSTRÖM, Mitglied der Europäischen Kommission • Rob WAINWRIGHT, Direktor von Europol • Blanche PETRE, Leitende SWIFT-Beraterin • Darius ŽILYS, Ratsvorsitz, Direktor der Abteilung für Völkerrecht, litauisches Justizministerium (Ko-Vorsitzender der Ad hoc-Arbeitsgruppe EU-USA zum Datenschutz) • Paul NEMITZ, Direktor GD JUST, Europäische Kommission (Ko-Vorsitzender der Ad hoc-Arbeitsgruppe EU-USA zum Datenschutz) • Reinhard PRIEBE, Direktor GD

	- Aussprache mit der US-Zivilgesellschaft (Teil I) - Wirksamkeit der Überwachung bei der Bekämpfung von Verbrechen und Terrorismus in Europa - Vorstellung der Studie über die Überwachungsprogramme der USA und ihre Auswirkungen auf die Privatsphäre der EU-Bürger	HOME, Europäische Kommission (Ko-Vorsitzender der Ad hoc-Arbeitsgruppe EU-USA zum Datenschutz) • Jens-Henrik JEPPESEN, Direktor für Europäische Angelegenheiten, Zentrum für Demokratie und Technology (CDT) • Greg NOJEIM, Leitender Jurist und Direktor des „Project on Freedom, Security & Technology“ (Projekt Freiheit, Sicherheit & Technologie), Zentrum für Demokratie und Technologie (CDT) (per Videokonferenz) • Dr. Reinhard KREISSL, Koordinator des EU-Projekts IRISS („Increasing Resilience in Surveillance Societies“ Stärkung der Widerstandskraft in Überwachungsgesellschaften) (per Videokonferenz) • Caspar BOWDEN, unabhängiger Forscher, ehemaliger leitender Datenschutzberater von Microsoft, Verfasser des Vermerks der Fachabteilung über die Überwachungsprogramme der USA und ihre Auswirkungen auf die Privatsphäre der EU-Bürger, der vom LIBE-Ausschuss in Auftrag gegeben wurde
30. September 2013 15.00 – 18.30 Uhr (Brüssel) **Mit AFET**	- Aussprache mit der US-Zivilgesellschaft (Teil II) - Tätigkeiten von Informanten im Bereich Überwachung und ihr rechtlicher Schutz	• Marc ROTENBERG, Electronic Privacy Information Centre (EPIC) • Catherine CRUMP, American Civil Liberties Union (ACLU) Stellungnahmen von Informanten: • Thomas DRAKE, ehemaliger Senior Executive der NSA • J. Kirk WIEBE, ehemaliger

		Senior analyst der NSA • Annie MACHON, ehemalige MI5-Agentin Stellungnahmen von NRO zum rechtlichen Schutz von Informanten: • Jesselyn RADACK, Rechtsanwältin und Vertreterin von sechs Informanten, Government Accountability Project • John DEVITT, Transparency International Ireland
3. Oktober 2013 16.00 – 18.30 Uhr (Brüssel)	- Verdacht des „Hackens“/Abhörens der Belgacom-Systeme durch Nachrichtendienste (GCHQ, Vereinigtes Königreich)	• Geert STANDAERT, Vizepräsident der Abteilung Service Delivery Engine, BELGACOM S.A. • Dirk LYBAERT, Generalsekretär, BELGACOM S.A. • Frank ROBBEN, „Commission de la Protection de la Vie Privée“ Belgien, Mitberichterstatter des „Belgacom-Dossiers“
7. Oktober 2013 19.00 – 21.30 Uhr (Straßburg)	- Auswirkungen der US-Überwachungsprogramme auf die US-Datenschutzgrundsätze des „sicheren Hafens“ - Auswirkungen der US-Überwachungsprogramme auf andere Instrumente des internationalen Transfers (Vertragsbestimmungen, verbindliche unternehmensinterne Vorschriften)	• Dr. Imke SOMMER, Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (DEUTSCHLAND) • Christopher CONNOLLY – Galexia • Peter HUNSTINX, Europäischer Datenschutzbeauftragter (EDSB) • **Isabelle FALQUE-PIERROTIN,** Präsidentin der französischen Datenschutzbehörde CNIL (FRANKREICH)
14. Oktober	- Elektronische	• Martin SCHEININ, ehemaliger

2013 15.00 – 18.30 Uhr (Brüssel)	Massenüberwachung von EU-Bürgern sowie auf internationaler Ebene, Europarat und EU-Recht - Gerichtsverfahren zu Überwachungsprogrammen	UN-Sonderberichterstatter zur Förderung und zum Schutz der Menschenrechte im Rahmen der Terrorismusbekämpfung, Professor am Europäischen Hochschulinstitut und Leiter des FP7-Projekts „SURVEILLE“ • Richter Bostjan ZUPANČIČ, Richter am Europäischen Gerichtshof für Menschenrechte (per Videokonferenz) • Douwe KORFF, Professor für Rechtswissenschaften, London Metropolitan University • Dominique GUIBERT, Vizepräsident der „Ligue des Droits de l'Homme“ (LDH) • Nick PICKLES, Direktor von Big Brother Watch • Constanze KURZ, Informatikerin, Projektleiterin beim Forschungszentrum für Kultur und Informatik
7. November 2013 9.00 – 11.30 Uhr und 15.00 – 18.30 Uhr (Brüssel)	- Die Rolle des EU INTCEN im Rahmen der Nachrichtendiensttätigkeit der EU (unter Ausschluss der Öffentlichkeit) - Nationale Programme zur Massenüberwachung personenbezogener Daten in den EU-Mitgliedstaaten und ihre Vereinbarkeit mit dem EU-Recht - Die Rolle der parlamentarischen Kontrolle der Nachrichtendienste auf nationaler Ebene im Zeitalter	• Ilkka SALMI, Direktor des EU-Zentrums für Informationsgewinnung und -analyse (INTCEN) • Dr. Sergio CARRERA, Senior Research Fellow und Leiter der Abteilung Justiz und Inneres, Zentrum für Europäische Politische Studien (CEPS), Brüssel • Dr. Francesco RAGAZZI, Assistenzprofessor für Internationale Beziehungen, Universität Leiden • Iain CAMERON, Mitglied der Europäischen Kommission für Demokratie durch Recht - „Venedig-Kommission“ • Ian LEIGH, Professor für

	der Massenüberwachung (Teil I)[1] (Venedig-Kommission) (Vereinigtes Königreich) - Transatlantische Expertengruppe EU-USA	Rechtswissenschaften, Universität Durham • David BICKFORD, Ehemaliger Justiziar der britischen Sicherheits- und Nachrichtendienste MI5 und MI6 • Gus HOSEIN, Geschäftsführer, Privacy International • Paul NEMITZ, Direktor - Grundrechte und Unionsbürgerschaft, GD JUST, Europäische Kommission • Reinhard PRIEBE, Direktor - Krisenmanagement und Innere Sicherheit, GD Home, Europäische Kommission
11. November 2013 15.00 – 18.30 Uhr (Brüssel)	- Überwachungsprogramme der USA und ihre Auswirkungen auf die Privatsphäre der EU-Bürger (Stellungnahme von Jim SENSENBRENNER, Mitglied im US-Kongress) - Die Rolle der parlamentarischen Kontrolle der Nachrichtendienste auf nationaler Ebene im Zeitalter der Massenüberwachung (NL, SW) (Teil II) - Programme der NSA zur elektronischen Massenüberwachung und die Rolle von IT-Unternehmen (Microsoft, Google, Facebook)	• Jim SENSENBRENNER, Mitglied des US-Repräsentantenhauses, (Mitglied im „Committee on the Judiciary“ (Rechtsausschuss) und Vorsitzender des „Subcommittee on Crime, Terrorism, Homeland Security, and Investigations“ (Unterausschuss für Verbrechensbekämpfung, Terrorismus, innere Sicherheit und Ermittlungen)) • Peter ERIKSSON, Vorsitzender des Verfassungsausschusses, Schwedisches Parlament (Riksdag) • A. H. VAN DELDEN, Vorsitzender des niederländischen unabhängigen Prüfungsausschusses für Nachrichten- und Sicherheitsdienste (CTIVD) • Dorothee BELZ, Vizepräsidentin, Rechts- und Unternehmensangelegenheiten

[1] Die Geheimdienst-Aufsichtsgremien von mehreren nationalen Parlamenten der EU wurden eingeladen, bei der Untersuchung als Zeugen auszusagen.

		Microsoft (Bereich Europa, Naher Osten und Afrika) • Nicklas LUNDBLAD, Direktor, Öffentlichkeitsarbeit und Regierungsbeziehungen, Google • Richard ALLAN, Direktor (Bereich Europa, Naher Osten und Afrika) Öffentlichkeitsarbeit, Facebook
14. November 2013 15.00 – 18.30 Uhr (Brüssel) **Mit AFET**	- IT-Sicherheit der EU-Institutionen (Teil I) (EP, COM (CERT-EU), (eu-LISA)) - Die Rolle der parlamentarischen Kontrolle der Nachrichtendienste auf nationaler Ebene im Zeitalter der Massenüberwachung (Teil III) (BE, DA)	• Giancarlo VILELLA, Generaldirektor, GD ITEC, Europäisches Parlament • Ronald PRINS, Direktor und Mitbegründer von Fox-IT • Freddy DEZEURE, Leiter der Task Force CERT-EU, GD DIGIT, Europäische Kommission • Luca ZAMPAGLIONE, Sicherheitsbeauftragter, eu-LISA • Armand DE DECKER, Stellvertretender Vorsitzender des belgischen Senats, Mitglied des Überwachungsausschusses und des „Intelligence Services Oversight Committee“ (Ausschuss für die Aufsicht der Nachrichtendienste) • Guy RAPAILLE, Vorsitzender des „Intelligence Services Oversight Committee“ (Comité R) • Karsten LAURITZEN, Mitglied des Rechtsausschusses, Sprecher für Rechtsangelegenheiten – Dänisches Folketing
18. November 2013 19.00 – 21.30 Uhr (Straßburg)	- Gerichtsverfahren und andere Beschwerden zu nationalen Überwachungsprogrammen (Teil II) (Polnische NRO)	• Dr. Adam BODNAR, Vizepräsident des Verwaltungsrats, Helsinki-Stiftung für Menschenrechte (Polen)
2. Dezember 2013 15.00 – 18.30 Uhr (Brüssel)	- Die Rolle der parlamentarischen Kontrolle der Nachrichtendienste auf nationaler Ebene im Zeitalter der Massenüberwachung (Teil IV)	• Michael TETZSCHNER, Mitglied des ständigen Überwachungs- und Verfassungsausschusses,

	(Norwegen)	Norwegen (Stortinget)
5. Dezember 2013, 15.00 – 18.30 Uhr (Brüssel)	- IT-Sicherheit der EU-Institutionen (Teil II) - Die Auswirkungen der Massenüberwachung auf die Vertraulichkeit in den Beziehungen zwischen Anwälten und Mandanten	• Olivier BURGERSDIJK, Head of Strategy, Europäisches Zentrum zur Bekämpfung der Cyberkriminalität, EUROPOL • Prof. Udo HELMBRECHT, Geschäftsführender Direktor der ENISA • Florian WALTHER, Unabhängiger Berater für IT-Sicherheit • Jonathan GOLDSMITH, Generalsekretär, Rat der Anwaltschaften der Europäischen Union (CCBE)
9. Dezember 2013 (Straßburg)	- Wiederherstellung des Vertrauens in die Datenübermittlung zwischen der EU und den USA - Entschließung des Europarats 1954 (2013) über nationale Sicherheit und Zugang zu Informationen	• Viviane REDING, Vizepräsidentin der Europäischen Kommission • Arcadio DÍAZ TEJERA, Mitglied des spanischen Senats, - Mitglied der Parlamentarischen Versammlung des Europarats und Berichterstatter für dessen Entschließung 1954 (2013) über nationale Sicherheit und Zugang zu Informationen
17.- 18. Dezember (Brüssel)	Parlamentarischer Untersuchungsausschuss über das Ausspionieren des brasilianischen Senats (Videokonferenz) Möglichkeiten der IT zum Schutz der Privatsphäre	• Vanessa GRAZZIOTIN, Vorsitzende des Parlamentarischen Untersuchungsausschusses über das Ausspionieren des brasilianischen Senats • Ricardo DE REZENDE FERRAÇO, Berichterstatter des Parlamentarischen Untersuchungsausschusses über das Ausspionieren des brasilianischen Senats • Bart PRENEEL, Professor für Computersicherheit und Industrielle Kryptographie an der Universität KU Leuven, Belgien • Stephan LECHNER, Direktor, Institut für Schutz und Sicherheit des Bürgers (IPSC), -

	Aussprache mit dem Journalisten, der die Fakten veröffentlicht hat (Teil II) (Videokonferenz)	Gemeinsame Forschungsstelle (JRC), Europäische Kommission • Dr. Christopher SOGHOIAN, Leitender Techniker, Projekt Sprache, Privatsphäre & Technologie, American Civil Liberties Union (Amerikanische Bürgerrechtsunion) • Christian HORCHERT, Berater für IT-Sicherheit, Deutschland • Glenn GREENWALD, Autor und Kolumnist, Spezialgebiet nationale Sicherheit und bürgerliche Freiheiten, ehemals bei The Guardian
22. Januar 2014 (Brüssel)	Meinungsaustausch über die russischen Abhörpraktiken bei Kommunikation (SORM) (Videokonferenz)	• Andrei Soldatov, investigativer Journalist, ein Herausgeber von Agentura.ru

ANHANG III: LISTE DER SACHVERSTÄNDIGEN, DIE DIE TEILNAHME AN DEN ÖFFENTLICHEN ANHÖRUNGEN DES LIBE-UNTERSUCHUNGSAUSSCHUSSES ABGELEHNT HABEN

1. Sachverständige, die die Einladung des LIBE-Vorsitzes abgelehnt haben

USA

- Keith Alexander, General der US-Armee, Direktor der NSA[1]
- Robert S. Litt, General Counsel (Leiter Rechtsangelegenheiten), Office of the Director of National Intelligence (Büro des Direktors der nationalen Nachrichtendienste)[2]
- Robert A. Wood, Geschäftsträger, Botschafter der Vereinigten Staaten bei der Europäischen Union

Vereinigtes Königreich

- Sir Iain Lobban, Direktor United Kingdom Government Communications Headquarters (GCHQ) (Kommunikationszentrum der britischen Regierung)

Frankreich

- Bernard Bajolet, Directeur général de la Sécurité Extérieure, Frankreich
- Patrick Calvar, Directeur Central de la Sécurité Intérieure, Frankreich

Deutschland

- Gerhard Schindler, Präsident des Bundesnachrichtendienstes

Niederlande

- Ronald Plasterk, Minister für Inneres und Königreichsbeziehungen, die Niederlande
- Ivo Opstelten, Minister für Sicherheit und Justiz, die Niederlande

Polen

- Dariusz Łuczak, Leiter der Agentur für innere Sicherheit, Polen
- Maciej Hunia, Leiter des polnischen Auslandsnachrichtendienstes

Private IT-Unternehmen

[1] Der Berichterstatter traf sich mit Keith Alexander und dem Vorsitzenden Elmar Brok sowie US-Senatorin Dianne Feinstein am 29. Oktober 2013 in Washington.
[2] Die Delegation des LIBE-Ausschusses traf sich am 29. Oktober 2013 mit Robert S. Litt in Washington.

- Tekedra N. Mawakana, Global Head of Public Policy (Leiterin der Öffentlichkeitsarbeit) und Deputy General Counsel (Stellvertretende Leiterin der Rechtsabteilung), Yahoo
- Dr. Saskia Horsch, Senior Manager Public Policy (Leitende Angestellte im Bereich Öffentlichkeitsarbeit), Amazon

Telekommunikationsunternehmen der EU

- Doutriaux, Orange
- Larry Stone, President Group Public & Government Affairs (Vorsitzender des Bereichs Öffentliche Angelegenheiten und Regierungsangelegenheiten des Konzerns) British Telecom, Vereinigtes Königreich
- Telekom, Deutschland
- Vodafone

2. Sachverständige, die nicht auf die Einladung des LIBE-Vorsitzes geantwortet haben

Niederlande

- Rob Bertholee, Directeur Algemene Inlichtingen en Veiligheidsdienst (AIVD)

Schweden

- Ingvar Åkesson, Schwedischer Nachrichtendienst
(Försvarets radioanstalt, FRA)

ERGEBNIS DER SCHLUSSABSTIMMUNG IM AUSSCHUSS

Datum der Annahme	12.2.2014
Ergebnis der Schlussabstimmung	+: 33 –: 7 0: 17
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Jan Philipp Albrecht, Roberta Angelilli, Mario Borghezio, Rita Borsellino, Arkadiusz Tomasz Bratkowski, Philip Claeys, Carlos Coelho, Agustín Díaz de Mera García Consuegra, Ioan Enciu, Frank Engel, Monika Flašíková Beňová, Kinga Gál, Kinga Göncz, Sylvie Guillaume, Salvatore Iacolino, Lívia Járóka, Teresa Jiménez-Becerril Barrio, Timothy Kirkhope, Juan Fernando López Aguilar, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Anthea McIntyre, Nuno Melo, Louis Michel, Claude Moraes, Antigoni Papadopoulou, Georgios Papanikolaou, Judith Sargentini, Birgit Sippel, Csaba Sógor, Rui Tavares, Axel Voss, Tatjana Ždanoka, Auke Zijlstra
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter(innen)	Alexander Alvaro, Anna Maria Corazza Bildt, Monika Hohlmeier, Stanimir Ilchev, Iliana Malinova Iotova, Jean Lambert, Marian-Jean Marinescu, Jan Mulder, Siiri Oviir, Salvador Sedó i Alabart
Zum Zeitpunkt der Schlussabstimmung anwesende Stellv. (Art. 187 Abs. 2)	Richard Ashworth, Phil Bennion, Françoise Castex, Jürgen Creutzmann, Christian Ehler, Knut Fleckenstein, Carmen Fraga Estévez, Nadja Hirsch, Maria Eleni Koppa, Evelyn Regner, Luis Yáñez-Barnuevo García, Gabriele Zimmer