EUROPÄISCHES PARLAMENT 2009 – 2014

*Ausschuss für bürgerliche Freiheiten, Justiz und Inneres*

**2013/2188(INI)**

8.1.2014

# ENTWURF EINES BERICHTS

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

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 die transatlantische 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 dessen 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),

– 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],

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

[1] http://www.un.org/en/documents/udhr/
[2] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement

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 Sicherheitsdienste2 und in Erwartung der im Frühjahr 2014 anstehenden Aktualisierung desselben mit regem Interesse,

– 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)196) und vom 20. Oktober 2004 (SEC(2004)1323) zu der Umsetzung der Grundsätze des „sicheren Hafens" zum Datenschutz,

– in Kenntnis der Mitteilung der Kommission vom 27. November 2013 (COM(2013)847) über das Funktionieren des sicheren Hafens aus Sicht der EU-

[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; 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.

Bürger und der in der EU niedergelassenen Unternehmen und der Mitteilung der Kommission vom 27. November 2013 (COM(2013)846) über die Wiederherstellung des Vertrauens in den Datenfluss zwischen der EU und den USA,

– unter Hinweis auf die Entschließung des Europäischen Parlaments 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, insbesondere Stellungnahme 4/20002,

– unter Hinweis auf die Abkommen zwischen der EU und den Vereinigten Staaten von Amerika 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)844),

– unter Hinweis auf die Stellungnahme von Generalanwalt Cruz Villalón, in der dieser folgerte, dass 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 unvereinbar ist[6],

– 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 Vereinigten Staaten von Amerika über Rechtshilfe[8],

---

[1] ABl. C 121 vom 24.4.2001, S. 152.
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32de.pdf
[3] ABl. L 204 vom 4.8.2007, S. 18.
[4] ABl. L 215 vom 11.8.2012, S. 5.
[5] SEC(2013) 630, 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.
[8] ABl. L 181 vom 19.7.2003, S. 34.

– 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[1],

– unter Hinweis auf die Erklärung des Präsidenten der Föderativen Republik Brasilien bei 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 US 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,

– unter Hinweis auf derzeit im US-Kongress zur Debatte stehende Legislativvorschläge, insbesondere den Entwurf des US Freedom Act,

– 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 Prüfgruppe des Präsidenten zu Nachrichtendienst und Kommunikationstechnik durchgeführten Überprüfungen, insbesondere auf den Bericht des 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 No 13-0851 vom 16. Dezember 2013,

– unter Hinweis auf den Bericht über die Ergebnisse der EU-Co-Vorsitzenden der Ad-hoc-Arbeitsgruppe der EU und der USA zum Datenschutz vom 27. November 2013[2],

– 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),

[1] ABl. L 309 vom 29.11.1996, S. 1.
[2] Ratsdokument 16987/13.

– unter Hinweis auf seine Entschließung vom 21. Mai 2013 über die EU-Charta: Normensetzung für die Freiheit der Medien in der EU[1],

– 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 untersuchen2,

– unter Hinweis auf seine Entschließung vom 23. Oktober 2013 zu organisiertem Verbrechen, Korruption und Geldwäsche: Empfohlene Maßnahmen und Initiativen[3],

– unter Hinweis auf seine Entschließung vom 23. Oktober 2013 zur Aussetzung des TFTP-Abkommens infolge der Überwachungsmaßnahmen der NSA4,

– unter Hinweis auf seine Entschließung vom 10. Dezember 2013 zur Freisetzung des Cloud-Computing-Potenzials in Europa[5],

– in Kenntnis der Interinstitutionellen Vereinbarung zwischen dem Europäischen 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 fallen6,

– gestützt auf Anhang VIII seiner Geschäftsordnung,

– gestützt auf Artikel 48 seiner Geschäftsordnung,

– in Kenntnis des Berichts des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (A70000/2013),

***Auswirkungen von Massenüberwachung***

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

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

C. in der Erwägung, dass die Welt im September 2001 in eine neue Phase eingetreten ist, was dazu führte, dass die Bekämpfung von Terrorismus zu den höchsten Prioritäten

[1] Angenommene Texte, P7_TA(2013)0203.
[2] Angenommene Texte, P7_TA(2013)0322.
[3] Angenommene Texte, P7_TA(2013)0444.
[4] Angenommene Texte, P7_TA(2013)0449.
[5] Angenommene Texte, P7_TA(2013)0535.
[6] ABl. C 353 E vom 3.12.2013, S.156-167.

der meisten Regierungen gehört; in der Erwägung, dass demokratisch gewählte Staats- und Regierungschefs infolge der Enthüllungen aufgrund durchgesickerter Dokumente des ehemaligen Mitarbeiters der NSA Edward Snowden verpflichtet sind, den Herausforderungen steigender Kapazitäten von Geheimdiensten bei Überwachungstätigkeiten sowie deren Auswirkungen auf die Rechtsstaatlichkeit in einer demokratischen Gesellschaft zu begegnen;

D. 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;
- das hohe Risiko der Verletzung von EU-Bestimmungen, Grundrechten und Datenschutzstandards;
- das Maß an Vertrauen zwischen den transatlantischen Partnern EU und USA;
- das Ausmaß der Zusammenarbeit mit und Beteiligung an Überwachungsprogrammen der USA oder gleichwertigen Programmen auf nationaler Ebene durch bestimmte EU-Mitgliedstaaten, das von den Medien enthüllt wurde;
- das Ausmaß an 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 strikten Bekämpfung des Terrorismus verwendet wird, etwa für Wirtschafts- und Industriespionage oder zur Profilerstellung aus politischen Gründen;
- die jeweiligen Rollen und der Grad der Beteiligung von Nachrichtendiensten und privaten IT- und Telekommunikationsunternehmen;
- die zunehmend verschwimmenden Grenzen zwischen Rechtsdurchsetzung und nachrichtendienstlichen Tätigkeiten, wodurch jeder Bürger als Verdächtiger behandelt wird;
- die Bedrohung der Privatsphäre in einer digitalen Ära;

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

F. in der Erwägung, dass die US-Behörden zwar einige der offenbarten Informationen bestreiten, die überwiegende Mehrheit allerdings nicht anfechten; in der Erwägung, dass sich die öffentliche Debatte in den USA und einigen EU-Mitgliedstaaten in großem Umfang entwickelt hat; in der Erwägung, dass die Regierungen der EU zu oft schweigen und es versäumen, angemessene Untersuchungen in Gang zu setzen;

G. 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 von EU-Verträgen nicht durch eine wegwerfende Inkaufnahme der extraterritorialen Auswirkungen der Aktivitäten oder Normen von Drittländern beeinträchtigt wird;

***Entwicklungen in den USA hinsichtlich der Reform der Nachrichtendienste***

H. 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 verstößt[1];

I. 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];

J. in der Erwägung, dass die Prüfgruppe des Präsidenten zu Nachrichtendienst und Kommunikationstechnik in ihrem Bericht vom 12. Dezember 2013 45 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-Personen gemäß § 215 des 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, die Beschwerden von Informanten entgegenzunehmen, für den Erhalt elektronischer Kommunikation bilaterale Rechtshilfeverträge einzusetzen und Überwachung nicht dazu zu verwenden, Betriebs- oder Handelsgeheimnisse zu stehlen;

K. in der Erwägung, dass in den Empfehlungen an den US-Präsidenten hinsichtlich nachrichtendienstlicher Aktivitäten gegen Nicht-US-Personen gemäß § 702 FISA das grundlegende Problem der Achtung der Privatsphäre und der Menschenwürde

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

anerkannt wird, die in Artikel 12 der Allgemeinen Menschenrechtserklärung und in Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte verankert ist; in der Erwägung, dass nicht empfohlen wird, Nicht-US-Personen die gleichen Rechte und den gleichen Schutz wie US-Personen zu gewähren;

***Rechtlicher Rahmen***

*Grundrechte*

L. in der Erwägung, dass der Bericht über die Ergebnisse der EU-Co-Vorsitzenden der Ad-hoc-Arbeitsgruppe der EU und der USA zum Datenschutz zwar einen Überblick über die rechtliche Situation in den USA gibt, jedoch nicht ausreichend dazu beigetragen hat, die Fakten zu Überwachungsprogrammen der USA zu ermitteln; in der Erwägung, dass es 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;

M. in der Erwägung, dass Grundrechte, insbesondere freie Meinungsäußerung, Pressefreiheit, Gedanken-, Gewissens-, Religions- und Versammlungsfreiheit, Privatleben, 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;

*Zuständigkeiten der Union im Bereich Sicherheit*

N. 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) über bestimmte Zuständigkeiten hinsichtlich der kollektiven Sicherheit der Union verfügt; in der Erwägung, dass die EU ihre Zuständigkeit hinsichtlich interner Sicherheit 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;

O. 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;

P. in der Erwägung, dass öffentliche oder nicht-öffentliche Stellen der Mitgliedstaaten, die im Bereich der nationalen Sicherheit tätig sind, unter der EMRK auch die hierin verankerten Rechte einhalten müssen, sei es in Bezug auf ihre eigenen Bürgerinnen und Bürger oder die Bürgerinnen und Bürger anderer Staaten; in der Erwägung, dass dies auch für die Zusammenarbeit mit den Behörden anderer Staaten im Bereich der

nationalen Sicherheit gilt;

*Extra-Territorialität*

Q. in der Erwägung, dass in den Situationen, die unter die Rechtsprechung der EU oder eines ihrer Mitgliedstaaten fallen, die extra-territoriale 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 außergewöhnlichen Umständen notwendig ist, Maßnahmen auf EU-Ebene zu ergreifen, um die Rechtsstaatlichkeit und die Einhaltung der Rechte natürlicher oder juristischer Personen in der EU sicherzustellen, insbesondere indem die Auswirkungen der betreffenden ausländischen Gesetzgebung beseitigt, ausgeglichen oder blockiert werden oder ihnen auf andere Wese entgegengewirkt wird;

***Internationale Datenübermittlung***

R. 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;

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

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

T. 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 Vereinigten Staaten zu übermitteln;

U. in der Erwägung, dass das Europäische Parlament in seiner Entschließung vom 5. Juli 2000 Zweifel und Bedenken an der Angemessenheit des sicheren Hafens ausgedrückt

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

und die Kommission aufgefordert hat, ihre Entscheidung vor dem Hintergrund von Erfahrungen und legislativer Entwicklungen zeitnah zu überprüfen;

V. in der Erwägung, dass in der Entscheidung 520/2000 der Kommission vorgesehen ist, 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 das unmittelbar bevorstehende Risiko eines schweren Schadens schaffen würde;

W. 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 dieser Entscheidung entsprechende Maßnahmen vorschlägt;

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

Y. 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;

Z. in der Erwägung, dass vom 28. bis 31. Oktober 2013 die 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;

AA. 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 werden 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 eine solche Ausnahme nicht auf eine Art angewendet werden sollte, durch die der vom EU-Datenschutzgesetz und den Grundsätzen des sicheren Hafens gewährte Schutz beeinträchtigt wird;

AB. in der Erwägung, dass das transatlantische Vertrauen durch den groß angelegten Zugriff von US-Nachrichtendiensten ernsthaft ausgehöhlt und das Vertrauen in 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*

AC. in der Erwägung, dass gemäß den enthüllten Informationen und den Ergebnissen der Überprüfung durch den LIBE-Ausschuss die nationalen Sicherheitsdienste Neuseelands und Kanadas 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 gegenseitig personenbezogene Daten von EU-Bürgern, die von der EU übermittelt wurden, ausgetauscht haben;

AD. in der Erwägung, dass das Schutzniveau, das seitens des Personal Information Protection and Electronic Documents Act Neuseelands und Kanadas sichergestellt wird, in den Entscheidungen der Kommission 2013/65[1] und 2/2002 vom 20. Dezember 2001[2] für angemessen befunden wurde; 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;

*Übermittlung auf Grundlage von Vertragsklauseln und anderen Instrumenten*

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

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

sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet;

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

AG. 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;

AH. 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 unmittelbar bevorstehende Risiko eines schweren Schadens schaffen würde;

AI. 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;

*Übermittlung auf Grundlage von TFTP- und PNR-Abkommen*

AJ. 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 Abkommen, insbesondere dessen Artikel 1, darstellen würde, Ausdruck verliehen hat;

AK. in der Erwägung, dass das Europäische 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;

AL. in der Erwägung, dass die Kommission nach den von den Medien veröffentlichten Behauptungen die Aufnahme von Konsultationen mit den USA gemäß Artikel 19 des TFTP-Abkommens beschlossen hat; in der Erwägung, dass Kommissar 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;

AM. in der Erwägung, dass die LIBE-Delegation in 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 vor dem LIBE-Untersuchungsausschuss angab, dass die NSA und die GCHQ SWIFT-Netze anvisiert hätten;

AN. 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 konnten1;

AO. 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 DHS an die NSA erfolgten;

AP. 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*

[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

*in Strafsachen*

AQ. in der Erwägung, dass das Abkommen zwischen der EU und den USA über Rechtshilfe in Strafsachen vom 6. Juni 20031 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")*

AR. 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;

AS. in der Erwägung, dass mit diesem Abkommen klare und eindeutige rechtsverbindliche Grundsätze für die Datenverarbeitung festgelegt werden sollen und insbesondere das Recht der EU-Bürger auf 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 und unabhängige Aufsicht der Datenverarbeitung anerkannt werden sollen;

AT. 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;

AU. 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***

AV. in der Erwägung, dass der rechtliche Rahmen 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

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

vorstellte, bestehend aus einer Datenschutzgrundverordnung[1], die die Richtlinie 95/46/EG 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;

AW. 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 Legislaturperiode verabschiedet werden;

AX. in der Erwägung, dass es dem Europäischen Rat – wenngleich er bei seinem Treffen 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 – nicht gelungen ist, einen allgemeinen Ansatz in Bezug auf die Datenschutzgrundverordnung und die Richtlinie zu finden3;

***IT-Sicherheit und Cloud-Computing***

AY. in der Erwägung, dass das Cloud-Computing-Geschäft laut der Entschließung vom 10. Dezember4 über ein bedeutendes Wachstums- und Beschäftigungspotenzial verfügt;

AZ. 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;

BA. 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 werden; in der Erwägung, dass die US-amerikanischen Geheimdienste auf personenbezogene Daten zugegriffen haben, die auf in der EU befindlichen Servern gespeichert sind, indem sie die internen Netze von Yahoo und Google anzapften[5]; in der Erwägung, dass derartige Aktivitäten eine Verletzung der internationalen Verpflichtungen 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;

***Demokratische Kontrolle der Geheimdienste***

BB. in der Erwägung, dass die Geheimdienste eine wichtige Rolle beim Schutz der

[1] COM(2012) 11 vom 25.1.2012.
[2] COM(2012) 10 vom 25.1.2012.
[3] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf
[4] AT-0353/2013 PE506.114V2.00.
[5] The Washington Post vom 31.10.2013.

demokratischen Gesellschaft gegen innere und äußere Bedrohungen spielen; in der Erwägung, dass ihnen zu diesem Zweck besondere Befugnisse und Kompetenzen verliehen wurden; in der Erwägung, dass sie von diesen Befugnissen innerhalb der Grenzen des Gesetzes Gebrauch machen müssen, da sie sonst Gefahr laufen, an Legitimität zu verlieren und das demokratische Wesen der Gesellschaft zu untergraben;

BC. in der Erwägung, dass der hohe Grad der Geheimhaltung, der bei Nachrichtendiensten erforderlich ist – um laufende Operationen nicht zu gefährden, Arbeitsweisen nicht preiszugeben oder das Leben von Agenten nicht in Gefahr zu bringen –, jedoch die vollständige Transparenz, öffentliche Überprüfung und normale demokratische oder juristische Untersuchung verhindert;

BD. in der Erwägung, dass die technischen Entwicklungen zu einer zunehmenden internationalen Zusammenarbeit im nachrichtendienstlichen Bereich, auch beim Austausch personenbezogener Daten, geführt haben, so dass sich häufig die Grenze zwischen nachrichtendienstlichen und polizeilichen Tätigkeiten verwischte;

BE. 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 technischen Fortschritte des letzten Jahrzehnts angepasst wurden;

BF. 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 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;

***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 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 Kommunikations-, 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 das britischen Geheimdienstes GCHQ, wie etwa das

Programm zur Überwachung der Kommunikation über transatlantische Glasfaserkabel (Tempora-Programm) und das Entschlüsselungsprogramm Edgehill; erachtet es als wahrscheinlich, dass ähnliche Programme, wenngleich in geringerem Umfang, auch in anderen EU-Ländern wie etwa Frankreich (DGSE), Deutschland (BND) und Schweden (FRA) vorhanden sind;

3. nimmt die Behauptungen zur Kenntnis, wonach der britische Geheimdienst GCHQ in die Systeme des Unternehmens Belgacom eingedrungen sein und diese angezapft haben soll; bekräftigt die Angaben von Belgacom, wonach das Unternehmen nicht bestätigen 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. stellt fest, dass das Vertrauen zwischen den beiden transatlantischen Partnern, das Vertrauen zwischen den EU-Mitgliedstaaten, das Vertrauen zwischen den Bürgern und ihren Regierungen, das Vertrauen in die Achtung der Rechtstaatlichkeit sowie das Vertrauen in die Sicherheit von IT-Dienstleistungen zutiefst erschüttert ist; ist der Meinung, dass es dringend eines umfassenden Plans 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; unterstützt ausdrücklich den Kampf gegen den Terrorismus, ist jedoch der festen Überzeugung, dass dieser Kampf an sich niemals als Rechtfertigung für ungezielte, geheime und mitunter sogar rechtswidrige Programme zur Massenüberwachung dienen kann; äußert daher seine Bedenken hinsichtlich der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit dieser Programme;

6. erachtet es als sehr bedenklich, 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 machtpolitische Motive wie politische Spionage oder Wirtschaftsspionage eine Rolle spielen könnten;

7. 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, wonach die Mitgliedstaaten alle Maßnahmen unterlassen, die die Verwirklichung der Ziele der Union gefährden könnten;

8. 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;

9. verurteilt aufs Schärfste die in gigantischem Ausmaß erfolgte systematische,

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 und das Recht auf freie Meinungsäußerung hin, sowie darauf, dass sie ein erhebliches Missbrauchspotential birgt, da die gesammelten Daten gegen politische Feinde eingesetzt werden könnten; betont, dass die beschriebenen Massenüberwachungsmaßnahmen scheinbar auch illegale Handlungen seitens der Geheimdienste einschließen und Fragen bezüglich der extraterritorialen Wirkung nationaler Gesetze aufwerfen;

10. erachtet die Überwachungsprogramme als weiteren Schritt hin zur Einrichtung eines echten Präventionsstaats, in dem ein Paradigmenwechsel des in demokratischen Gesellschaften etablierten Strafrechts erfolgt und stattdessen eine Mischung aus Strafverfolgungs- und Geheimdienstaktivitäten propagiert wird, die unklaren 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;

11. weist mit Nachdruck darauf hin, dass geheime Gesetze, Verträge und Gerichte eine Verletzung der Rechtsstaatlichkeit darstellen; betont, dass die Urteile von Gerichten und die Entscheidungen von Verwaltungsbehörden in Nicht-EU-Staaten, die Überwachungsmaßnahmen ähnlich den in dieser Untersuchung betrachteten direkt oder indirekt genehmigen, nicht automatisch anerkannt oder vollstreckt werden dürfen, sondern jeweils nach den entsprechenden nationalen Verfahren für gegenseitige Anerkennung und Rechtshilfe und den Bestimmungen bilateraler Abkommen zu behandeln sind;

12. weist darauf hin, dass die genannten Befürchtungen durch die rasche technische und gesellschaftliche Entwicklung noch verstärkt werden; vertritt die Auffassung, dass es sich um ein Problem bisher ungekannten Ausmaßes handelt, 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 aller Art basiert, die eine Gefahr für die Integrität der betroffenen Person darstellt;

13. erachtet es als eindeutige, von den im Rahmen der Untersuchung aussagenden IT-Experten betonte Erkenntnis, dass weder die öffentlichen Institutionen noch die Bürger der EU beim derzeitigen technischen Entwicklungsstand sicher sein können, dass ihre IT-Systeme und ihre Privatsphäre vor Eingriffen durch gut ausgerüstete

[1] Nr. 1 BvR 518/02 vom 4.4.2006.

Geheimdienste aus Drittstaaten oder EU-Ländern geschützt sind („keine 100%-ige IT-Sicherheit“); stellt fest, dass diese beunruhigende Situation nur dann überwunden werden kann, wenn man in Europa bereit ist, ausreichende personelle und finanzielle Mittel für die Aufrechterhaltung der Unabhängigkeit und Eigenständigkeit bereitzustellen;

14. weist die Auffassung, dass diese Fragen lediglich die nationale Sicherheit betreffen und daher ausschließlich der Zuständigkeit der Mitgliedstaaten unterliegen, mit Nachdruck zurück; 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 und der Souveränität der EU sind;

15. begrüßt die Diskussionen, die derzeit in verschiedenen Teilen der Welt um den Gegenstand dieser Untersuchung geführt werden, sowie die diesbezüglichen Untersuchungen und Überprüfungen; weist auf den von den weltweit führenden Technologieunternehmen unterzeichneten Aufruf zu einer „Global Government Surveillance Reform“ (Globale Reform der staatlichen Überwachung) hin, mit dem grundlegende Veränderungen in den einzelstaatlichen Überwachungsgesetzen – darunter ein internationales Verbot der Sammelerhebung von Daten – gefordert werden, damit das Vertrauen der Öffentlichkeit in das Internet erhalten bleibt; nimmt die vor kurzem veröffentlichten Empfehlungen der vom US-Präsidenten eingesetzten Review Group on Intelligence and Communications Technologies 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 der Geheimdienste so zu überarbeiten, dass sie angemessene Schutzmaßnahmen und Kontrollmechanismen vorsehen;

16. spricht seine Anerkennung für die Institutionen und Experten aus, die zu dieser Untersuchung beigetragen haben; 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;

17. 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 Legislaturperiode, die sicherstellen sollen, dass die Erkenntnisse ganz oben auf der politischen Agenda der EU bleiben;

[1] Nr. 1 BvR 518/02 vom 4.4.2006.

18. beabsichtigt, von der nach den Wahlen im Mai 2014 ernannten Kommission ehrgeizige politische Zusagen für eine Umsetzung der Vorschläge und Empfehlungen dieser Untersuchung zu verlangen; erwartet von den Kandidaten, dass sie in den bevorstehenden Anhörungen der neuen Kommissionsmitglieder im Europäischen Parlament ein entsprechendes Engagement erkennen lassen;

***Empfehlungen***

19. fordert die US-Behörden und die EU-Mitgliedstaaten auf, die pauschale Massenüberwachung und Massenverarbeitung personenbezogener Daten zu verbieten;

20. fordert bestimmte EU-Mitgliedstaaten, darunter das Vereinigte Königreich, Deutschland, Frankreich, Schweden und die Niederlande auf, ihre nationalen Rechtsvorschriften und Verfahren im Bereich geheimdienstlicher Tätigkeiten erforderlichenfalls zu überarbeiten, um sicherzustellen, dass diese mit den Normen der Europäischen Menschenrechtskonvention sowie mit ihren aus den Grundrechten erwachsenden Verpflichtungen hinsichtlich Datenschutz, Privatsphäre und Unschuldvermutung in Einklang stehen; betont angesichts der ausführlichen Medienberichte über Massenüberwachung im Vereinigten Königreich insbesondere, dass der derzeitige rechtliche Rahmen, 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, überarbeitet werden sollte;

21. fordert die Mitgliedstaaten auf, 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;

22. fordert die Mitgliedstaaten auf, unverzüglich ihrer positiven Verpflichtung im Rahmen der Europäischen Menschenrechtskonvention nachzukommen, wonach sie ihre Bürger vor Überwachungsmaßnahmen durch Drittstaaten, 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;

23. 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“;

24. 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 EU-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;

25. 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 und das Zusatzprotokoll des IPBPR zu unterzeichnen, das Beschwerden durch Einzelpersonen ermöglicht;

26. spricht sich vehement gegen die Unterzeichnung eines Zusatzprotokolls oder von Leitlinien über den grenzüberschreitenden Zugriff auf gespeicherte Computerdaten zum Übereinkommen über Computerkriminalität (Budapester Konvention) des Europarats aus, da dies den unautorisierten, bestehende Instrumente der gegenseitigen Rechtshilfe außer Acht lassenden Zugriff von Geheimdiensten auf Daten, die in anderen Gerichtsbarkeiten gespeichert sind, legitimieren und zu einem ungehinderten Fernzugriff von Strafverfolgungsbehörden auf Server und Computersysteme in anderen Gerichtsbarkeiten führen könnte und dem Übereinkommen des Europarats Nr. 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zuwiderliefe;

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

***Internationale Datenübermittlungen***

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

28. 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 (Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); erklärt sich besorgt über das Eingeständnis dieser Unternehmen, dass sie den Informations- und Kommunikationsfluss zwischen ihren Datenzentren nicht verschlüsseln, wodurch sie den Geheimdiensten das Abfangen von Informationen ermöglichen[1];

29. 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 per se die Kriterien für eine Ausnahmeregelung aus Gründen der „nationalen Sicherheit" erfüllt;

[1] The Washington Post vom 31.10.2013.

30. 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, die konkrete Sicherheits- und Schutzmaßnahmen vorsehen;

31. 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;

32. fordert die zuständigen Behörden der Mitgliedstaaten, namentlich 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, sofern diese die nötigen Sicherheits- und Schutzbestimmungen für den Schutz der Privatsphäre sowie der Grundrechte und Freiheiten von Personen enthalten;

33. fordert die Kommission auf, bis Juni 2014 eine umfassende Bewertung des rechtlichen Rahmens der USA für den Schutz der Privatsphäre vorzulegen, die Handels-, Strafvollzugs- und Geheimdienstaktivitäten beurteilt, um so auf die Tatsache zu reagieren, dass die Rechtssysteme der EU und der USA im Bereich des Schutzes personenbezogener Daten auseinander driften;

*Übermittlungen in andere Drittstaaten aufgrund von Entscheidungen über die Angemessenheit*

34. 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;

35. erinnert daran, dass laut Richtlinie 95/46/EG die Angemessenheit des Schutzniveaus, das ein Drittland bietet, unter Berücksichtigung aller Umstände beurteilt wird, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen 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, während sie laut Richtlinie 95/46/EG ebenfalls befugt ist, festzustellen, dass ein Drittland kein angemessenes Schutzniveau gewährleistet;

36. 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 Abhilfe für die festgestellte Lage zu schaffen;

37. fordert die Kommission und die Mitgliedstaaten auf, unverzüglich zu prüfen, ob die in den Entscheidungen der Kommission 2013/65/EU1 vom 19. Januar 2012 bzw. 2002/2/EG vom 20. Dezember 2001 festgestellte Angemessenheit des Datenschutzniveaus in Neuseeland und des Datenschutzes, den der kanadische „Personal Information Protection and Electronic Documents Act“ (Gesetz über personenbezogene Informationen und elektronische Dokumente) bietet, durch die Beteiligung der Geheimdienste Neuseelands und Kanadas 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; erwartet von der Kommission, dass sie dem Europäischen 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*

38. 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 Abweichklauseln zu den Vertragsklauseln oder verbindlichen unternehmensinternen Vorschriften entspreche, die sich auf außergewöhnliche Abweichungen aus berechtigtem Interesse in einer demokratischen Gesellschaft, sofern erforderlich und angemessen, beziehen;

39. 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 feststeht, dass der Datenimporteur nach den für ihn geltenden Rechtsvorschriften Anforderungen unterliegt, die über die in einer demokratischen Gesellschaft erforderlichen Beschränkungen hinausgehen und sich wahrscheinlich sehr nachteilig auf die Garantien auswirken werden, die das anwendbare Datenschutzrecht und die Standardvertragsklauseln bieten, oder wenn die Fortsetzung der Datenübermittlung den betroffenen Personen einen unmittelbar bevorstehenden schweren Schaden zuzufügen droht;

40. fordert die Artikel-29-Datenschutzgruppe 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;

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

41. fordert die Kommission auf, 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*

42. 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 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 Protokoll 36 und dessen Artikel 10 sowie Erklärung 50 zu diesem Protokoll berücksichtigt werden;

*EU-Rechtshilfe in Strafsachen*

43. ersucht den Rat und die Kommission, das Parlament darüber zu informieren, inwiefern das Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten, insbesondere Titel III zur Überwachung des Telekommunikationsverkehrs, von den Mitgliedstaaten tatsächlich angewandt wird; fordert die Kommission auf, wie beantragt vor Ende 2014 in Übereinstimmung mit Erklärung 50 zu 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*

44. 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;

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

46. 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")*

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

48. fordert die umgehende Wiederaufnahme der Verhandlungen mit den USA zu dem „Rahmenabkommen", das klare Rechte der EU-Bürger sowie gültige und durchsetzbare administrative und gerichtliche Rechtsbehelfe in den USA ohne jegliche Diskriminierung gewährleisten soll;

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

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

*Datenschutzreform*

51. fordert den Vorsitz im Rat und die Mehrzahl der Mitgliedstaaten, die ein hohes Datenschutzniveau unterstützen, auf, eine Führungsrolle zu übernehmen, Verantwortungsbewusstsein zu zeigen und ihre Arbeiten am gesamten Datenschutzpaket voranzutreiben, sodass eine Annahme im Jahr 2014 ermöglicht wird, damit die EU-Bürger in sehr naher Zukunft von einem besseren Schutz profitieren können;

52. betont, dass sowohl die Datenschutzvorschrift als auch die Datenschutzrichtlinie zum Schutz der Grundrechte des Einzelnen notwendig sind und daher 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;

*Cloud-Computing*

53. 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 als wesentliches Element für Wachstum und Beschäftigung sowie für das Vertrauen in Cloud-Computing-Dienste und -Anbieter und für die Sicherung eines hohen Schutzniveaus für personenbezogene Daten hervor;

54. 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 bezüglich des direkten Fernzugriffs auf personenbezogene Daten und Informationen durch die Strafverfolgungsbehörden und Nachrichtendienste von

Drittstaaten;

55. bekundet sein Bedauern darüber, 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;

56. appelliert an die Kommission und die Mitgliedstaaten, die Arbeit an der Europäischen Cloud-Partnerschaft zu beschleunigen;

57. weist darauf hin, dass alle Unternehmen, die in der EU Dienstleistungen anbieten, ausnahmslos die Rechtsvorschriften der EU einhalten und für etwaige Rechtsverstöße haften müssen;

*Abkommen über die transatlantische Handels- und Investitionspartnerschaft (TTIP)*

58. stellt fest, dass die EU und die USA Verhandlungen bezüglich einer transatlantischen Handels- und Investitionspartnerschaft führen, die von großer strategischer Bedeutung für weiteres Wirtschaftswachstum und die Fähigkeit der EU und der USA ist, künftige globale Regulierungsstandards festzulegen;

59. hebt angesichts der Bedeutung der digitalen Wirtschaft in der Beziehung und bei der Wiederherstellung des Vertrauens zwischen der EU und den USA besonders hervor, dass das Europäische Parlament dem endgültigen TTIP-Abkommen nur zustimmen wird, wenn darin die von der EU-Charta anerkannten Grundrechte in vollem Umfang respektiert werden, und dass der Schutz der Privatsphäre des Einzelnen im Zusammenhang mit der Verarbeitung und Verbreitung personenbezogener Daten weiterhin durch Artikel XIV des GATS geregelt werden muss;

***Demokratische Aufsicht über Nachrichtendienste***

60. 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;

61. ersucht wie im Falle von Echelon alle nationalen Parlamente, die dies noch nicht getan haben, 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 für eine effektive Kontrolle der Nachrichtendienste verfügen;

62. fordert die Bildung einer hochrangigen Gruppe zur Stärkung der Kooperation auf dem Gebiet der Nachrichtendienste auf EU-Ebene, in Kombination mit einem geeigneten Aufsichtsmechanismus, der sowohl die demokratische Legitimität als auch die

entsprechende technische Leistungsfähigkeit sicherstellt; betont, dass die hochrangige Gruppe eng mit den nationalen Parlamenten zusammenarbeiten sollte, um weitere Schritte für eine stärkere Zusammenarbeit in der EU im Bereich der Aufsicht vorzuschlagen;

63. fordert diese hochrangige Gruppe auf, 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) zu definieren;

64. fordert die hochrangige Gruppe auf, die Dauer jeder angeordneten Überwachung strikt zu begrenzen, sofern deren Fortsetzung nicht ordnungsgemäß durch die Genehmigungs-/Aufsichtsbehörde begründet wird;

65. fordert die hochrangige Gruppe auf, Kriterien für mehr Transparenz auf der Grundlage des Grundprinzips der Informationsfreiheit und der sogenannten „Tshwane-Prinzipien“1 zu entwickeln;

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

67. 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;

68. 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);

69. fordert die Kommission dringend auf, bis September 2014 einen Vorschlag für eine Rechtsgrundlage für die Tätigkeit des EU-Zentrums für Informationsgewinnung und -analyse (IntCen) sowie für einen dessen Tätigkeiten gerechten Aufsichtsmechanismus mit regelmäßiger Berichterstattung an das Europäische Parlament vorzulegen;

70. fordert die Kommission auf, bis September 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;

[1] The Global Principles on National Security and the Right to Information, June 2013.

71. erinnert an die Bestimmungen der Interinstitutionellen Vereinbarung zwischen dem Europäischen 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, die zur Verbesserung der Aufsicht auf EU-Ebene verwendet werden sollten;

***Agenturen der Europäischen Union***

72. 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;

73. fordert Europol auf, die zuständigen Behörden der Mitgliedstaaten zu ersuchen, nach Maßgabe ihrer Befugnisse Untersuchungen zu möglicher Cyberkriminalität und Cyberangriffen seitens Regierungen oder privater Akteure im Zuge der zu prüfenden Tätigkeiten einzuleiten;

***Recht auf freie Meinungsäußerung***

74. äußert seine tiefe Sorge über die aufkommenden 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“;

75. vertritt die Auffassung, dass 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) eine Beeinträchtigung des Rechts der freien Meinungsäußerung gemäß Artikel 10 EMRK und Artikel 11 der EU-Charta darstellt;

76. fordert die Kommission auf, einen Vorschlag zu einem umfassenden Rahmenwerk für den Informantenschutz in der EU vorzubringen und dabei besonders auf die Besonderheiten der Meldung von Missständen im Bereich der Nachrichtendienste einzugehen, für die sich die Bestimmungen zur Meldung von Missständen im Finanzbereich möglicherweise als unzureichend erweisen, und weitreichende Immunitätszusicherungen miteinzubeziehen;

***IT-Sicherheit in der EU***

77. 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 deutlich machen; stellt fest, dass für diese Angriffe eine finanzielle und personelle Ausstattung in einem Umfang erforderlich ist, dass sie wahrscheinlich von staatlichen Einrichtungen im Auftrag von ausländischen Regierungen oder bestimmten nationalen Regierungen in der EU ausgehen, welche diese unterstützen; versteht in diesem Zusammenhang den Hacking- und Spähangriff auf das Telekommunikationsunternehmen Belgacom als besorgniserregendes Beispiel eines Angriffs auf die IT-Kapazitäten der EU;

78. 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 mittelfristig autonome IT-Schlüsselkapazitäten aufzubauen; 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;

79. ist äußerst besorgt über die Hinweise, dass Auslandsgeheimdienste versucht haben, die IT-Sicherheitsstandards zu senken und Backdoors („Hintertüren“) in vielen verschiedenen IT-Systemen zu installieren;

80. fordert alle Mitgliedstaaten, die Kommission, den Rat und den Europäischen Rat auf, den gefährlichen Mangel der EU an Autonomie in Bezug auf IT-Werkzeuge, -Unternehmen und -Anbieter (Hardware, Software, Dienstleistungen und Netze) sowie Verschlüsselungskapazitäten und kryptografische Möglichkeiten zu beheben;

81. fordert die Kommission, Normungsgremien und ENISA auf, bis September 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 besser zu schützen; ist der Überzeugung, dass diese Standards in einem offenen und demokratischen Verfahren festgelegt werden sollten, das nicht von einem einzelnen Land, einer einzelnen Einrichtung oder einem multinationalen Unternehmen vorangetrieben wird; 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;

82. weist darauf hin, dass Telekommunikationsunternehmen und die EU sowie nationale Regulierungsbehörden für Telekommunikation 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 Verschlüsselung der Kommunikation gefordert wird;

83. unterstützt die Cybersicherheitsstrategie der EU, ist jedoch der Ansicht, dass diese nicht alle potenziellen Bedrohungen abdeckt und dass sie auf gefährliche Verhaltensweisen von Staaten ausgedehnt werden sollte;

84. 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);

85. fordert die Kommission auf, im nächsten Arbeitsprogramm des Rahmenprogramms „Horizont 2020“ zu bewerten, ob mehr Mittel für die Förderung der europäischen Forschung, Entwicklung, Innovation und Schulung im Bereich der IT-Technologien eingesetzt werden sollten, vor allem für Technologien und Infrastrukturen für einen besseren Datenschutz, Verschlüsselung, sichere Datenverarbeitung, quelloffene Sicherheitslösungen und die Informationsgesellschaft;

86. fordert die Kommission auf, die gegenwärtigen Zuständigkeiten im Einzelnen festzulegen und bis spätestens Juni 2014 den Bedarf für ein umfassenderes Mandat, eine bessere Koordination und/oder zusätzliche Mittel und technische Kapazitäten für das Europäische Zentrum zur Bekämpfung der Cyberkriminalität von Europol, ENISA, CERT-EU und den EDSB zu prüfen, damit diese schwerwiegende Verletzungen der IT-Sicherheit in der EU wirksamer untersuchen und technische Untersuchungen im Zusammenhang mit schwerwiegenden Verletzungen vor Ort durchführen (oder Mitgliedstaaten und EU-Organe bei der Durchführung unterstützen) können;

87. hält es für erforderlich, dass die EU von einer eigenen IT-Akademie unterstützt wird, in der die besten europäischen Fachleute in allen damit zusammenhängenden Fachgebieten zusammengeführt werden und die Aufgabe erhalten, allen einschlägigen Gemeinschaftsorganen und -einrichtungen wissenschaftliche Beratung zu IT-Technologien, u. a. zu sicherheitsbezogenen Strategien, bereitzustellen; fordert die Kommission auf, zunächst ein unabhängiges wissenschaftliches Expertengremium einzurichten;

88. fordert das Generalsekretariat des Europäischen Parlaments auf, bis spätestens September 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 EP ein hohes Maß an Sicherheit zu erreichen; ist der Auffassung, dass eine solche Bewertung mindestens die Analyse von Informationen und Empfehlungen zu Folgendem umfassen muss:

- den Bedarf an regelmäßigen, strengen, 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;

- die Liste der US-Unternehmen, die beim Europäischen Parlament im IT- und Telekommunikationsbereich unter Vertrag stehen, unter Berücksichtigung der 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;

- die Zuverlässigkeit und Belastbarkeit von kommerzieller Software von Dritten, die von den Gemeinschaftsorganen in ihren IT-Systemen verwendet wird, in Bezug auf das Eindringen von Strafverfolgungs- und Geheimdienstbehörden von EU-Staaten oder Drittländern;

- die Verwendung von mehr quelloffenen Systemen und weniger serienmäßig produzierten kommerziellen Systemen;

- die Auswirkungen des verstärkten Einsatzes von mobilen Geräten (Smartphones, Tablets, unabhängig vom beruflichen oder privaten Gebrauch) und dessen Auswirkungen auf die IT-Sicherheit des Systems;

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

- die Verwendung und die Standorte von Servern und IT-Zentren für das IT-System des EP 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-Sicherung durch das EP, einschließlich der in der Cloud gesicherten Arten von Daten, wie die Inhalte und der Zugriff geschützt sind und wo sich die Cloud befindet, um das für den Datenschutz geltende Rechtssystem zu klären;

- 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 einer elektronischen Signatur in E-Mails;

- eine Analyse der Vorteile bei der Verwendung von GNU Privacy Guard als vorgegebenen Verschlüsselungsstandard für E-Mails, mit dem gleichzeitig die Verwendung digitaler Signaturen möglich wäre;

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

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

90. 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 Haushaltsplanentwurf für das Jahr 2015 zugewiesen werden müssen;

91. ist der Ansicht, dass die IT-Großsysteme im Raum der Freiheit, der Sicherheit und des Rechts, wie das Schengener Informationssystems der zweiten Generation, das Visa-Informationssystem, Eurodac und mögliche zukünftige Systeme auf eine Weise entwickelt und betrieben werden sollten, durch die sichergestellt wird, dass die Datensicherheit nicht durch Anfragen vonseiten der USA gemäß Patriot Act gefährdet wird; fordert eu-LISA auf, dem Parlament bis Ende 2014 Bericht über die Zuverlässigkeit der bestehenden Systeme zu erstatten;

92. fordert die Kommission und den EAD auf, Maßnahmen auf internationaler Ebene, insbesondere bei den VN, und in Zusammenarbeit mit interessierten Partnern (wie Brasilien) zu ergreifen, und eine EU-Strategie für die demokratische Regierungsführung in Bezug auf das Internet umzusetzen, um 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 wird;

93. fordert, dass die gesamte Architektur des Internets hinsichtlich Datenflüssen und Datensicherung neu überdacht wird, wobei mehr Datensparsamkeit und Transparenz und weniger die zentrale Massenspeicherung von Rohdaten angestrebt werden und die unnötige Verlegung von Datenverkehr auf Hoheitsgebiete von Ländern vermieden wird, welche die grundlegenden Standards hinsichtlich Grundrechten, Datenschutz und Privatsphäre nicht einhalten;

94. fordert die Mitgliedstaaten auf, in Zusammenarbeit mit ENISA, dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität von Europol, den CERT, den nationalen Datenschutzbehörden und den Dienststellen zur Bekämpfung der

Cyberkriminalität 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, einschließlich mithilfe von „digitaler Hygiene“, Verschlüsselung und sicherem Cloud-Computing, wobei die in der Universaldienstrichtlinie vorgesehenen Plattformen für Informationen von allgemeinem Interesse umfassend genutzt werden;

95. fordert die Kommission auf, bis September 2014 Möglichkeiten zu bewerten, um die Software- und Hardwarehersteller zur Integration von mehr Sicherheit und Datenschutz über Standardfunktionen in ihren Produkten anzuhalten, einschließlich der Möglichkeit, eine gesetzliche Haftung seitens der Hersteller für nicht behobene, bekannte Schwachstellen oder die Installation von geheimen Backdoors („Hintertüren“) einzuführen und negative Anreize für die unzulässige und unverhältnismäßige Massensammlung von persönlichen Daten zu setzen sowie gegebenenfalls Gesetzgebungsvorschläge vorzulegen;

***Wiederherstellung des Vertrauens***

96. ist überzeugt, dass die Untersuchung gezeigt hat, dass die USA das Vertrauen ihrer Partner wiedererlangen müssen, da es in erster Linie um die Aktivitäten der US-Geheimdienste geht;

97. 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 Rechtsstaatlichkeit und die Glaubwürdigkeit der demokratischen Garantien in einer digitalen Gesellschaft;

*Zwischen der EU und den USA*

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

99. ist der Überzeugung, dass die Massenüberwachung von Bürgerinnen und Bürgern und die Ausspähung von politischen Führungskräften 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. Diese Umstände werden 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;

100. 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 fortgesetzt wird; fordert jedoch 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;

101. 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 auf Privatsphäre angesprochen wird, die gleichen Rechte auf Auskunft und Schutz der Privatsphäre in den US-Gerichten garantiert werden und die derzeitige Diskriminierung nicht fortgesetzt wird;

102. 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 durch eindeutig festgelegte Bedingungen beschränkt ist und mit einem hinreichenden Verdacht oder hinreichenden Tatverdacht auf terroristische oder kriminelle Aktivitäten zusammenhängt; betont, dass diese Zwecke einer transparenten gerichtlichen Kontrolle unterliegen müssen;

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

104. 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;

105. ermuntert die 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 hat, und auf diese Weise die gemeinsame Rechtsgrundlage der transatlantischen Verbündeten zu stärken;

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

*Innerhalb der Europäischen Union*

107. ist zudem der Ansicht, dass die Beteiligung und Aktivitäten von Mitgliedstaaten der

EU zu einem Vertrauensverlust 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 Stärkung der gerichtlichen und parlamentarischen Kontrolle, das verlorene Vertrauen wiederherstellen können;

108. ist sich der Tatsache bewusst, dass einige Mitgliedstaaten der EU eine bilaterale Kommunikation mit den US-Behörden anstrengen und dass einige von ihnen sogenannte „Anti-Spionage-Abkommen“ abgeschlossen haben (Vereinigtes Königreich) oder dessen Abschluss planen (Deutschland, Frankreich); betont, dass diese Mitgliedstaaten den Interessen der EU als Ganzes gerecht werden müssen;

109. ist der Ansicht, dass solche Abkommen nicht gegen europäische Verträge, insbesondere nicht gegen den Grundsatz der loyalen Zusammenarbeit (gemäß Artikel 4 Absatz 3 EUV) verstoßen oder EU-Strategien im Allgemeinen, konkret den Binnenmarkt, den lauteren Wettbewerb und die wirtschaftliche, industrielle und soziale Entwicklung, untergraben sollten; 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;

*International*

110. fordert die Kommission auf, spätestens im Januar 2015 eine EU-Strategie für demokratische Regierungsführung in Bezug auf das Internet vorzulegen;

111. fordert die Mitgliedstaaten auf, dem Ruf 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 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 Hohe Vertreterin/Vizepräsidentin der Kommission und den Auswärtigen Dienst auf, eine aktive Haltung einzunehmen;

112. 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 VN-Generalversammlung (Menschenrechtsausschuss) am 27. November 2013 verabschiedet wurde;

***Vorrangiges Programm: Ein europäischer digitaler Habeas-Corpus-Grundsatz***

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

114. beschließt, *einen europäischen digitalen Habeas-Corpus-Grundsatz für den Schutz*

*der Privatsphäre* auf der Grundlage der folgenden sieben Aktionen mit dem Europäischen Parlament als Aufsicht einzuführen:

Aktion 1: Annahme des Datenschutzpakets im Jahr 2014;

Aktion 2: Abschluss des Rahmenabkommens zwischen der EU und den USA, um ordnungsgemäße Rechtsbehelfsmechanismen für EU-Bürgerinnen und -Bürger 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 ordnungsgemäß ausgeräumt wurden;

Aktion 5: Schutz der Rechtsstaatlichkeit und der Grundrechte der Bürgerinnen und Bürger der EU, mit besonderem Schwerpunkt auf den Gefahren für Pressefreiheit und Berufsgeheimnis (einschließlich der Beziehungen zwischen Anwälten und Mandanten) sowie auf dem besseren Schutz für Informanten („Whistleblower");

Aktion 6: Entwickeln einer europäischen Strategie für die Unabhängigkeit der IT (auf nationaler und EU-Ebene);

Aktion 7: Entwicklung der EU als Maßstab für eine demokratische und neutrale Regierungsführung in Bezug auf das Internet;

115. fordert die Gemeinschaftsorgane und die Mitgliedstaaten auf, den europäischen digitalen Habeas-Corpus-Grundsatz zu unterstützen und zu fördern; verpflichtet sich, als Wächter über die Rechte der Bürgerinnen und Bürger der EU 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 den Medien in Bezug auf den Untersuchungsauftrag und die Prüfung der Umsetzung dieser Entschließung;

- ab Juli 2014: ein ständiger Aufsichtsmechanismus für Datenübermittlungen und Rechtsbehelfe im zuständigen Ausschuss;

- Frühjahr 2014: formelle Aufforderung an den Europäischen Rat, den europäischen digitalen Habeas-Corpus-Grundsatz in die gemäß Artikel 68

AEUV zu beschließenden Leitlinien aufzunehmen;

- Herbst 2014: Verpflichtung, dass der europäische digitale Habeas-Corpus-Grundsatz und die damit zusammenhängenden Empfehlungen bei der Bestätigung der nächsten Kommission als Schlüsselkriterium dienen werden;

- 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 Brasilien;

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

- 2015: 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;

116. 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 Mandat1 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 Information 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 Novelle „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 zueigen 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 Cyber-Angriffen durch Behörden von Ländern mit niedrigerem Demokratiestandard ergeben. Immer mehr wird man sich darüber 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 der persönlichen 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. Dieser Tage 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 Legislaturperiode 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:

**Eine digitale Habeas-Corpus-Akte zum Schutz der Privatsphäre, die sich auf sieben Handlungen stützt:**

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

Handlung 2: Abschluss eines Rahmenabkommens zwischen der EU und den USA, das EU-Bürgern für den Fall der Weitergabe von Daten durch die EU an die USA zu Zwecken der Strafverfolgung angemessene Rechtsbehelfsmechanismen gewährleistet;

Handlung 3: Aussetzung der Safe-Harbour-Regelung, bis eine umfassende Überprüfung erfolgt und bestehende Gesetzeslücken in einer Weise geschlossen werden, die sicherstellt, dass die Weitergabe personenbezogener Daten zu kommerziellen Zwecken aus der EU an die USA nur im Einklang mit höchsten EU-Standards erfolgen kann;

Handlung 4: Aussetzung des TFTA-Abkommens bis i) die Verhandlungen über das Rahmenabkommen abgeschlossen sind; ii) eine gründliche Untersuchung auf Grundlage der EU-Analyse durchgeführt worden ist und darin alle vom Parlament in dessen Entschließung vom 23. Oktober geäußerten Bedenken angemessen berücksichtigt worden sind;

Handlung 5: Schutz der Rechtsstaatlichkeit und der Grundrechte der EU-Bürger, mit besonderem Augenmerk auf die Bedrohung der Pressefreiheit und des Berufsgeheimnisses (einschließlich der Beziehungen zwischen Anwalt und Mandant) sowie einem erweiterten Schutz für Whistleblower;

Handlung 6: Entwicklung einer europaweiten Strategie zur Schaffung von Unabhängigkeit im IT-Bereich (sowohl auf einzelstaatlicher als auch auf EU-Ebene);

Handlung 7: Entwicklung der EU zu einem beispielgebenden Handlungsträger, der auf eine demokratische und neutrale Internet-Governance hinwirkt;

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

verfolgen:

- April - Juli 2014: ein auf dem LIBE-Untersuchungsteam gründendes Aufsichtsgremium, das für die Verfolgung jeglicher neuer in das Untersuchungsmandat fallender Enthüllungen in den Medien zuständig ist und die Umsetzung der vorliegenden Entschließung genau prüft;

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

- Frühjahr 2014: ein förmlicher Aufruf an den Rat, die Europäische Digitale Habeas-Corpus-Akte in die nach Artikel 68 AEUV zu verabschiedenden Richtlinien aufzunehmen;

- Herbst 2014: eine Selbstverpflichtung, dass die nächste Kommission ihre Zustimmung von der Europäischen Digitalen Habeas-Corpus-Akte und den zugehörigen Empfehlungen als zentralen Kriterien abhängig macht;

- 2014 - 2015: eine mit dem Themenkomplex Vertrauen/Daten/Bürgerrechte betraute Gruppe, die in regelmäßigen Abständen zwischen dem Europäischen Parlament und dem US-Kongress sowie mit Parlamenten beteiligter Drittländer, darunter Brasilien, einberufen wird;

- 2014 - 2015: eine Konferenz mit Gremien der europäischen einzelstaatlichen Parlamente zur Kontrolle der Nachrichtendienste;

- 2015: eine Konferenz, die hochrangige europäische Experten auf verschiedenen der IT-Sicherheit zuarbeitenden Gebieten (wie Mathematik, Kryptographie, Technologien für einen besseren Datenschutz) vereint, als Beitrag zur Entwicklung einer IT-Strategie der EU für die kommende Legislaturperiode;

## ANHANG I: LISTE DER ARBEITSDOKUMENTE

**LIBE-Untersuchungsausschuss**

| **Berichterstatter & Schattenberichterstatter 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" (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) |

## 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<br>• Jacob APPELBAUM, investigativer Journalist, Softwareentwickler und Spezialist für Computersicherheit beim Tor-Projekt<br>• 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<br>• Gerhard SCHMID (ehemaliges MdEP und Berichterstatter des ECHELON-Berichts im Jahr 2001)<br>• Duncan CAMPBELL, investigativer Journalist und Verfasser des STOA-Berichts |

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

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

| | | |
|---|---|---|
| | | • Annie MACHON, ehemalige MI5-Agentin<br><br>Stellungnahmen von NRO zum rechtlichen Schutz von Informanten:<br>• Jesselyn RADACK, Rechtsanwältin und Vertreterin von sechs Informanten, Government Accountability Project<br>• John DEVITT, Transparency International Ireland |
| 3. Oktober 2013<br>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.<br>• Dirk LYBAERT, Generalsekretär, BELGACOM S.A.<br>• 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“<br><br>- 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)<br>• Christopher CONNOLLY – Galexia<br>• Peter HUNSTINX, Europäischer Datenschutzbeauftragter (EDSB)<br><br>• **Isabelle FALQUE-PIERROTIN,** Präsidentin der französischen Datenschutzbehörde CNIL (FRANKREICH) |
| 14. Oktober 2013 15.00 – | - Elektronische Massenüberwachung von EU- | • Martin SCHEININ, ehemaliger UN-Sonderberichterstatter zur |

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

| | | |
|---|---|---|
| | (Venedig-Kommission)<br>(Vereinigtes Königreich)<br><br><br><br><br><br>- Transatlantische Expertengruppe EU-USA | Universität Durham<br>• David BICKFORD, Ehemaliger Justiziar der britischen Sicherheits- und Nachrichtendienste MI5 und MI6<br>• Gus HOSEIN, Geschäftsführer, Privacy International<br><br>• Paul NEMITZ, Direktor - Grundrechte und Unionsbürgerschaft, GD JUST, Europäische Kommission<br>• Reinhard PRIEBE, Direktor - Krisenmanagement und Innere Sicherheit, GD Home, Europäische Kommission |
| 11. November 2013<br>15.00 – 18.30 Uhr<br>(Brüssel) | - Überwachungsprogramme der USA und ihre Auswirkungen auf die Privatsphäre der EU-Bürger (Stellungnahme von Jim SENSENBRENNER, Mitglied im US-Kongress)<br><br><br>- Die Rolle der parlamentarischen Kontrolle der Nachrichtendienste auf nationaler Ebene im Zeitalter der Massenüberwachung (NL, SW) (Teil II)<br><br><br><br><br>- 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))<br><br>• Peter ERIKSSON, Vorsitzender des Verfassungsausschusses, Schwedisches Parlament (Riksdag)<br>• A. H. VAN DELDEN, Vorsitzender des niederländischen unabhängigen Prüfungsausschusses für Nachrichten- und Sicherheitsdienste (CTIVD)<br><br>• Dorothee BELZ, Vizepräsidentin, Rechts- und Unternehmensangelegenheiten Microsoft (Bereich Europa, Naher Osten und Afrika)<br>• Nicklas LUNDBLAD, Direktor, |

| | | |
|---|---|---|
| | | Öffentlichkeitsarbeit und Regierungsbeziehungen, Google<br>• Richard ALLAN, Direktor (Bereich Europa, Naher Osten und Afrika) Öffentlichkeitsarbeit, Facebook |
| 14. November 2013 15.00 – 18.30 Uhr (Brüssel)<br>**Mit AFET** | - IT-Sicherheit der EU-Institutionen (Teil I) (EP, COM (CERT-EU), (eu-LISA))<br><br>- 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<br>• Ronald PRINS, Direktor und Mitbegründer von Fox-IT<br>• Freddy DEZEURE, Leiter der Task Force CERT-EU, GD DIGIT, Europäische Kommission<br>• Luca ZAMPAGLIONE, Sicherheitsbeauftragter, eu-LISA<br><br>• Armand DE DECKER, Stellvertretender Vorsitzender des belgischen Senats, Mitglied des Überwachungsausschusses und des „Intelligence Services Oversight Committee“ (Ausschuss für die Aufsicht der Nachrichtendienste)<br>• Guy RAPAILLE, Vorsitzender des „Intelligence Services Oversight Committee“ (Comité R)<br>• 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) (Norwegen) | • Michael TETZSCHNER, Mitglied des ständigen Überwachungs- und Verfassungsausschusses, Norwegen (Stortinget) |
| 5. Dezember 2013, 15.00 – | - IT-Sicherheit der EU-Institutionen (Teil II) | • Olivier BURGERSDIJK, Head of Strategy, Europäisches |

| | | |
|---|---|---|
| 18.30 Uhr (Brüssel) | - Die Auswirkungen der Massenüberwachung auf die Vertraulichkeit in den Beziehungen zwischen Anwälten und Mandanten | Zentrum zur Bekämpfung der Cyberkriminalität, EUROPOL<br>• Prof. Udo HELMBRECHT, Geschäftsführender Direktor der ENISA<br>• Florian WALTHER, Unabhängiger Berater für IT-Sicherheit<br>• 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<br><br>- Entschließung des Europarats 1954 (2013) über nationale Sicherheit und Zugang zu Informationen | • Viviane REDING, Vizepräsidentin der Europäischen Kommission<br><br>• Arcadio DÍAZ TEJERA, Mitglied des spanischen Senats, - Mitglied der Parlamentarischen Versammlung des Europarats und Berichterstatter von dessen Entschließung 1954 (2013) über nationale Sicherheit und Zugang zu Informationen |
| 17.-18. Dezember (Brüssel) | Parlamentarischer Untersuchungsausschuss über das Ausspionieren des brasilianischen Senats (Videokonferenz)<br><br>Möglichkeiten der IT zum Schutz der Privatsphäre | • Vanessa GRAZZIOTIN, Vorsitzende des Parlamentarischen Untersuchungsausschusses über das Ausspionieren des brasilianischen Senats<br>• Ricardo DE REZENDE FERRAÇO, Berichterstatter des Parlamentarischen Untersuchungsausschusses über das Ausspionieren des brasilianischen Senats<br><br>• Bart PRENEEL, Professor für Computersicherheit und Industrielle Kryptographie an der Universität KU Leuven, Belgien<br>• Stephan LECHNER, Direktor, Institut für Schutz und Sicherheit des Bürgers (IPSC), - Gemeinsame Forschungsstelle (JRC), Europäische Kommission<br>• Dr. Christopher SOGHOIAN, |

| | | |
|---|---|---|
| | Aussprache mit dem Journalisten, der die Fakten veröffentlicht hat (Teil II) (Videokonferenz) | Leitender Techniker, Projekt Sprache, Privatsphäre & Technologie, American Civil Liberties Union (Amerikanische Bürgerrechtsunion)<br>• Christian HORCHERT, Berater für IT-Sicherheit, Deutschland<br>• Glenn GREENWALD, Autor und Kolumnist, Spezialgebiet nationale Sicherheit und bürgerliche Freiheiten, ehemals bei The Guardian |

## 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

**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**

- 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**

[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.

- 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**

**Deutschland**

- Gerhard Schindler, Präsident des Bundesnachrichtendienstes

**Niederlande**

- Berndsen-Jansen, Voorzitter Vaste Kamer Commissie voor Binnenlandse Zaken Tweede Kamer der Staten-Generaal, die Niederlande
- Rob Bertholee, Directeur Algemene Inlichtingen en Veiligheidsdienst (AIVD)

**Schweden**

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