EUROPÄISCHES PARLAMENT

GENERALDIREKTION INTERNE POLITIKBEREICHE

FACHABTEILUNG C
BÜRGERRECHTE UND KONSTITUTIONELLE ANGELEGENHEITEN

Konstitutionelle Fragen

Freiheit, Sicherheit und Justiz

Gleichstellung der Geschlechter

Rechts- und Parlamentarische Angelegenheiten

Petitionen

Die Überwachungsprogramme der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger

THEMENPAPIER

DE EN, FR

2013

EUROPEAN PARLIAMENT

GENERALDIREKTION INTERNE POLITIKBEREICHE

FACHABTEILUNG C:

BÜRGERRECHTE UND KONSTITUTIONELLE ANGELEGENHEITEN

BÜRGERLICHE FREIHEITEN, JUSTIZ UND INNERES

Die Überwachungsprogramme der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger

THEMENPAPIER

Kurzfassung

Im Lichte der jüngsten Enthüllungen im Zusammenhang mit dem Programm PRISM werden in diesem Themenpapier die Auswirkungen der Überwachungsprogramme der USA auf die Grundrechte der EU-Bürger analysiert. Gegenstand der Betrachtung sind **der Umfang der nach dem US-amerikanischen Gesetz von 2008 zur Änderung des Foreign Intelligence Surveillance Act (FISA) zulässigen Überwachung und die diesbezüglichen Praktiken der US-Behörden, die sich stark auf die Datenhoheit der EU und den Schutz der Rechte der europäischen Bürger auswirken.**

Das vorliegende Dokument wurde vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres in Auftrag gegeben.

VERFASSER

Caspar BOWDEN (Unabhängiger Datenschutzexperte)

Einleitung von Prof. Didier BIGO
(King's College London /
Direktor des *Centre d'Etudes sur les Conflits, Liberté et Sécurité* – CCLS, Paris (Frankreich).

Lektorat: Dr. Amandine SCHERRER
(*Centre d'Etudes sur les Conflits, Liberté et Sécurité* – CCLS, Paris (Frankreich)

Bibliografische Zuarbeit: Wendy Grossman

ZUSTÄNDIGER BEAMTER

Alessandro DAVOLI
Fachabteilung – Bürgerrechte und Konstitutionelle Angelegenheiten
Europäisches Parlament
B-1047 Brüssel
E-Mail: alessandro.davoli@europarl.europa.eu

SPRACHFASSUNGEN

Original: EN
Translation: DE, FR

ÜBER DEN HERAUSGEBER

Kontakt zur Fachabteilung oder Bestellung des monatlichen Newsletters: poldep-citizens@europarl.europa.eu

Redaktionsschluss: September 2013.

Dieses Dokument ist im Internet unter folgender Adresse abrufbar:
http://www.europarl.europa.eu/committees/de/studies.html

HAFTUNGSAUSSCHLUSS

INHALT

ABKÜRZUNGSVERZEICHNIS

ACLU	American Civil Liberties Union (Amerikanische Bürgerrechtsunion)
AUMF	Authorization to Use Military Force (Genehmigung des Einsatzes militärischer Gewalt)
CIA	Central Intelligence Agency (Zentraler Nachrichtendienst)
CNIL	Comité National pour l'Informatique et les Libertés (nationale Datenschutzbehörde Frankreichs)
DSB	Datenschutzbehörden
EDSB	Europäischer Datenschutzbeauftragter
ENISA	Europäische Agentur für Netz- und Informationssicherheit
FAA	Foreign Intelligence Surveillance Amendments Act (2008) (Gesetz zur Änderung des Gesetzes über die Überwachung der Auslandsgeheimdienste)
FBI	Federal Bureau of Investigation (Bundesamt für Ermittlung)
FIVE EYES	Vereinigtes Königreich, USA, Kanada, Australien, Neuseeland: Austausch von Geheimdienstinformationen im Rahmen der UKUSA-Vereinbarung
FISA	Foreign Intelligence Surveillance Act (1978) (Gesetz über die Überwachung der Auslandsgeheimdienste)
FISC	Foreign Intelligence Surveillance Court (Gericht für die Überwachung der Auslandsgeheimdienste)
FISCR	Foreign Intelligence Surveillance Court of Review (Revisionsgericht für die Überwachung der Auslandsgeheimdienste)
NSA	National Security Agency (Nationale Sicherheitsagentur)
PAA	Protect America Act (2007) (Gesetz zum Schutz Amerikas)

SHA „Safe Harbour“-Abkommen (2000) zwischen der EU und den USA

TIA Programm „Total Information Awareness“ (Totale Informationswahrnehmung)

WP29 Artikel-29-Datenschutzgruppe

ZUSAMMENFASSUNG

In diesem Themenpapier werden dem Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) Hintergrund- und Kontextinformationen zu den Tätigkeiten im Rahmen von PRISM/FISA/NSA und zu den Überwachungsprogrammen der USA sowie ihren konkreten Auswirkungen auf die Grundrechte der EU-Bürger, einschließlich des Rechts auf Privatsphäre und den Schutz personenbezogener Daten, zur Verfügung gestellt.

Vor dem PRISM-Skandal hatten die europäischen Medien diesen Aspekt unterschätzt, da sie offensichtlich verkannten, dass die Überwachungstätigkeit in erster Linie nicht auf US-Bürger, sondern auf den Rest der Welt ausgerichtet war. In dem Papier wird argumentiert, dass **der Umfang der Überwachung nach dem *Gesetz zur Änderung des Gesetzes über die Überwachung der Auslandsgeheimdienste von 2008* (FAA) weit reichende Folgen für die Datenhoheit der EU und den Schutz der Rechte ihrer Bürger hat.**

Der erste Abschnitt enthält einen **geschichtlichen Abriss der Überwachungsprogramme der USA**, der erkennen lässt, dass die US-Behörden das Menschenrecht von Nichtamerikanern auf Privatsphäre durchgehend missachtet haben. Aus der Analyse verschiedener Überwachungsprogramme (Echelon, PRISM) und der US-Rechtsvorschriften zur inneren Sicherheit (FISA, PATRIOT und FAA) geht klar hervor, dass die US-Behörden Überwachungsaktivitäten durchführen, ohne dabei die Rechte von Nicht-US-Bürgern und nicht in den USA ansässigen Personen zu beachten. Insbesondere der Geltungsbereich des FAA ermächtigt zu einer Massenüberwachung speziell von Daten im Ausland befindlicher nichtamerikanischer Bürger, darunter Daten, die im „Cloud Computing“ verarbeitet werden, das nicht unter die EU-Datenschutzvorschriften fällt.

Der zweite Abschnitt bietet einen**Überblick über die wichtigsten rechtlichen Lücken, Schlupflöcher und Kontroversen im Zusammenhang mit diesen Programmen und deren unterschiedlichen Folgen für die Rechte von US- und EU-Bürgern**. Dabei werden die Rechtsvorschriften zu den Überwachungsprogrammen der USA und weitere Unsicherheiten in Bezug auf ihre Anwendung erläutert, etwa:

- gravierende Einschränkungen des 4. Zusatzartikels zur US-Verfassung für US-Bürger
- spezielle Befugnisse hinsichtlich des Kommunikationsverkehrs und der personenbezogenen Daten von „Nicht-US-Personen“
- Fehlen erkennbarer Rechte auf Privatsphäre für „Nicht-US-Personen“ im Rahmen des FISA

Ferner geht aus dem Abschnitt hervor, dass der immer rascher zunehmende und bereits weitverbreitete Einsatz von Cloud Computing den Schutz der Daten von EU-Bürgern weiter untergräbt und dass eine Bestandsaufnahme einiger der bestehenden und geplanten Mechanismen, die die Rechte von EU-Bürgern nach der Weitergabe von Daten schützen sollen, ergeben hat, dass diese tatsächlich als Schlupflöcher wirken.

Schließlich werden einige**Strategieoptionen für das Europäische Parlament herausgearbeitet** und entsprechende Empfehlungen unterbreitet, die der Verbesserung künftiger EU-Vorschriften dienen und wirksame Garantien für den Schutz der Rechte von EU-Bürgern bieten sollen.

EINLEITUNG

Hintergrund

Mit diesem Themenpapier sollen dem LIBE-Ausschuss Hintergrund- und Kontextinformationen zu den Tätigkeiten im Rahmen von PRISM/FISA/NSA und zu Überwachungsprogrammen der USA sowie ihren Auswirkungen auf die Grundrechte der EU-Bürger, einschließlich des Rechts auf Privatsphäre und den Schutz personenbezogener Daten, zur Verfügung gestellt werden.

Am 5. Juni veröffentlichten die*Washington Post* und der *Guardian* einen Geheimbefehl nach Abschnitt 215 des USA PATRIOT Act (Gesetz zur Stärkung und Einigung Amerikas durch Bereitstellung geeigneter Instrumente, um Terrorismus aufzuhalten und zu blockieren), der von der Telefongesellschaft Verizon verlangte, der NSA Einzelheiten über alle innerhalb der USA getätigten und internationalen Telefongespräche zur Verfügung zu stellen, und zwar „laufend". Am 6. Juni enthüllten die beiden Zeitungen die Existenz eines NSA-Programms mit dem Decknamen PRISM, das auf Daten führender Internetkonzerne der USA zugriff. Noch am selben Tag bestätigte Admiral Clapper (NSA-Direktor) offiziell, dass PRISM bestehe und sich auf Befugnisse nach Abschnitt 702 (oder Paragraf 1881a) des FAA von 2008 stütze. Am 9. Juni gab Edward Snowden in einem Videointerview freiwillig seine Identität preis.

In der Entschließung des Europäischen Parlaments vom 4. Juli 2013 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten zeigten sich die Mitglieder des Parlaments sehr besorgt über PRISM und andere Überwachungsprogramme, verurteilten scharf das Ausspionieren von offiziellen Vertretern der EU und forderten die US-Behörden auf, der EU ohne weitere Umschweife sämtliche Informationen zu diesen Behauptungen zur Verfügung zu stellen. Untersuchungen werden derzeit auch von der Kommission[1], der WP29[2]und einigen Parlamenten der Mitgliedstaaten geführt.

Grenzüberschreitende Massenüberwachung und Demokratie – eine Problembetrachtung[3]

Die Enthüllungen Snowdens über PRISM machen deutlich, dass grenzüberschreitende elektronische Massenüberwachung zu systematischen Verstößen gegen Grundrechte führt. In Anbetracht dieser Verstöße sehen wir uns veranlasst, Fragen zum Umfang der grenzüberschreitenden Massenüberwachung und ihren Folgen für unsere Demokratien zu stellen.

> *„Geheimdienste der Art, wie sie in Polizeistaaten entstanden sind, werden von unserer Regierung von Natur aus und unserer offenen Gesellschaft aus tiefstem Instinkt im Einklang mit der Verfassung und den Zusatzartikeln automatisch geächtet."* (Allen Dulles, 1963)[4]

[1] EU-Kommissionsmitglied Viviane Reding (2013), Schreiben an den Generalstaatsanwalt, Zeichen Ares (2013)1935546 – 10/06/2013, Brüssel, 10. Juni 2013.
[2] Datenschutzgruppe nach Artikel 29, Schreiben des Vorsitzenden an Viviane Reding betreffend das Programm PRISM 13. August 2013.
[3] Vorbemerkung von Prof. Didier Bigo
[4] Dulles, Allen Welsh (1963), The Craft of Intelligence, New York: Harper&Row, S. 257.

„Spionage gibt es seit Jahren, überwacht wird auch schon seit Jahren und so weiter. Ich werde nicht darüber urteilen. Das liegt in der Natur unserer Gesellschaft."

(Eric Schmidt, Vorstandsvorsitzender von Google, 2013)

Zwischen diesen beiden Zitaten liegen 50 Jahre. Sie unterscheiden sich in der Antwort, betreffen aber dieselbe zentrale Frage: Wie lange können demokratische Gesellschaften als solche weiterbestehen, wenn geheimdienstliche Aktivitäten auch eine Massenüberwachung der Bevölkerung umfassen? Wie den Worten Eric Schmidts und den meisten Medienberichten der Welt zu entnehmen ist, hat sich die Gesellschaft ihrem Wesen nach gewandelt. Telekommunikationstechnologien wie die Mobiltelefonie, das Internet und die Satellitentechnik und im weiteren Sinne alle Daten, die sich digital erfassen und in Plattformen zusammenführen lassen, haben es möglich gemacht, bislang ungekannte Mengen von Daten zu sammeln, zu speichern, zu organisieren und zu durchsuchen. Wenn die Technologien existieren, so müssen sie genutzt werden: „Man kann nicht gegen den Strom schwimmen." Die Entdeckung, dass diese Techniken bei den von den Nachrichtendiensten betriebenen Programmen insgeheim genutzt und ihre Möglichkeiten voll ausgeschöpft werden, kommt daher nicht überraschend. Wenn alle anderen, die über diese technischen Mittel verfügen, sie auch nutzen – so die Denkweise – sollten wir das ebenfalls tun. Wenn nicht, wäre das naiv oder, schlimmer noch, eine Niederlage, die die innere Sicherheit eines Landes gefährdet, indem zugelassen wird, dass ein anderes Land sich die von diesen Technologien gebotenen Möglichkeiten zunutze macht.

Sollten wir jedoch mit dieser Ausweitung der Spionage auf die Massenüberwachung der Bevölkerung leben müssen und sie als gegeben hinnehmen? Glücklicherweise sind totalitäre Regime mehr oder weniger verschwunden, bevor das Potenzial dieser Mittel voll ausgeschöpft wurde. Wenn diese Technologien heute in demokratischen Grundordnungen zum Einsatz kommen, dann geschieht das zweckgebunden und dient in erster Linie der Zusammenarbeit bei der Terrorismusbekämpfung mit dem Ziel, Attentatsversuche zu verhindern. Den Nachrichtendiensten in aller Welt zufolge stellen diese Technologien keine Gefährdung für die bürgerlichen Freiheiten dar; sie seien das beste Mittel, die Bürger vor dem globalen Terrorismus zu schützen. Die Geheimdienste würden verdächtiges Verhalten untersuchen und Informationen auf internationaler Ebene austauschen. Prinzipiell stünden nur „echte Verdächtige" unter Beobachtung. Aus dieser Perspektive ließen sich die Enthüllungen über Programme wie PRISM ganz und gar nicht als Makel, sondern als Beweis für gut abgestimmte Zusammenarbeit ansehen, die künftig auf zahlreiche andere Formen der Gewalt ausgeweitet werden müsse.

Angesichts dieses von den wichtigsten Gremien der Geheimdienste und der Organisationen zur Terrorismusbekämpfung in den USA, im Vereinigten Königreich, in Frankreich und auf EU-Ebene angeführten „Erwägungsgrunds" ist es unerlässlich, das angeblich neue Wesen unserer Gesellschaft zu erörtern. Wie wirkt sich der Wandel der Technologien auf demokratische Gesellschaften aus, wie lassen sich diese Technologien als Mittel sowohl für den Informationsaustausch als auch für den Wettbewerb um Informationen (ein Schlüsselelement einer globalisierten Welt) einsetzen, welche Rechte haben die Regierungen bei der Verarbeitung dieser Informationen: So lauten die Kernfragen.

Wie von Allen Dulles oben festgestellt, leisten die von den Nachrichtendiensten angegebenen Begründungen dem Polizeistaat Vorschub und richten sich im Kern gegen eine offene, in einer demokratischen Grundordnung verankerte Gesellschaft. Die Verfechter einer offenen Gesellschaft bestehen entgegen dem früheren Trend darauf, dass Technologien nicht als Triebkraft für Handlungen des Menschen dienen sollten; sie müssten auf sinnvolle Weise und nach den Grundsätzen des Rechtsstaats eingesetzt werden. Die massive Überwachung muss eingedämmt werden. Die verfassungsrechtlichen Bestimmungen müssen angewendet werden, und die Unschuldsvermutung gilt für alle

Menschen (nicht nur Staatsangehörige). Wenn Verdachtsmomente bestehen, dann müssen sie bestimmte Formen der Kriminalität betreffen, nicht jedoch abweichendes Verhalten oder einen Lebensstil. Auf dem Spiel stehen hier also nicht die Mechanismen, die die Gesetze und Aktivitäten zur Terrorismusbekämpfung auf transatlantischer Ebene regeln, auch wenn sie einen Teilaspekt der Frage berühren. Ebenso wenig geht es um Aktivitäten der Spionage zwischen Regierungen. **Vielmehr geht es um die Frage, in welcher Art, welchem Ausmaß und welcher Tiefe eine Ausspähung innerhalb von und zwischen Demokratien hingenommen werden kann.**

Snowdens Enthüllungen deuten auf zahlreiche Grundrechtsverstöße hin. Sie betreffen in erster Linie alle Personen, deren Daten durch die Überwachung ihres Kommunikationsverkehrs, über Digitalkabel oder mittels Cloud-Computing-Technologien abgeschöpft wurden, sobald sie unter eine Verdachtskategorie fielen oder auf andere Weise von Interesse für Auslandsgeheimdienste waren. Diese Personen genießen jedoch nicht alle denselben Schutz, vor allem dann nicht, wenn sie keine US-Bürger sind. **EU-Bürger sind daher in dieser Konstellation aus US-Nachrichtendiensten, globale Dienste erbringenden Privatfirmen und den Eigentumsrechten, die jene über ihre Daten ausüben können, besonders verwundbar.** Zweifelsohne fallen EU-Bürger, wenn sie nicht dasselbe Maß an Schutz wie US-Bürger genießen, aufgrund der Praktiken der US-Nachrichtendienste und des Fehlens wirksamer Schutzmechanismen diesen Systemen als Erste zum Opfer. Gedankenfreiheit, Meinungsfreiheit, das Recht auf freie Meinungsäußerung und Pressefreiheit sind Grundwerte, die gewahrt werden müssen. Jeder Bürger der EU hat das Recht auf ein Privatleben, d. h. ein Leben, das nicht voll unter der Überwachung eines Staatsapparats steht. Die Regierungen müssen bei ihrem ermittlerischen Blick deutlich an die Unterscheidung zwischen privaten und öffentlichen Aktivitäten, zwischen Verbrechen und einem lediglich anderen Lebensstil erinnert werden. Mit der massenhaften Sammlung von Daten über den Lebensstil zum Zweck der Erstellung von Mustern und Profilen politischer Einstellungen und wirtschaftlicher Entscheidungen hat PRISM offenbar eine Beschaffung geheimdienstlicher Informationen in einem Ausmaß und einer Tiefe ermöglicht, die zuvor ungekannt waren und über die von liberalen Regierungen in der Vergangenheit durchgeführte Terrorismusbekämpfung und Spionagetätigkeit hinausgehen. Daraus kann eine illegale Form von „Totaler Informationswahrnehmung“ entstehen, bei der Daten von Millionen von Menschen in die Hände der NSA gelangen und von ihr ausgewertet werden.

In diesem Papier soll dieser Frage mit einem Blick auf die Praxis der geheimdienstlichen Aufklärung und ihre notwendigen Grenzen innerhalb von und zwischen Demokratien nachgegangen werden. Wie wir anhand der von Snowden vorgelegten Dokumente erkennen werden, ist das Ausmaß des Programms PRISM global; seine Erfassungstiefe erstreckt sich auf die digitalen Daten weiter Teile der Bevölkerung und verstößt gegen die Grundrechte großer Bevölkerungsgruppen, insbesondere der EU-Bürger. Die EU-Organe haben daher das Recht und die Pflicht, diese neue elektronische Massenüberwachung und ihre Auswirkungen auf die Grundrechte von EU-Bürgern im Ausland und in der Heimat zu untersuchen.

Regelungen zur Wahrung der Privatsphäre: Konkurrierende Modelle EU/USA

Eine sorgfältige Vergleichsanalyse der US-Gesetze zum Schutz der Privatsphäre und des EU-Datenschutzrahmens ergibt, dass die US-Gesetze dem Einzelnen wenige praktische Optionen bieten, sein Leben unter Wahrung des Rechts auf informationelle Selbstbestimmung zu gestalten. Eine wesentliche Folge des Datenschutzrechts besteht jedoch darin, dass bei einer Übertragung von Daten zwischen Computern, sofern die entsprechenden gesetzlichen Voraussetzungen erfüllt sind, der Einzelne keinen Einwand mit

der Begründung erheben kann, das Risiko für seine Privatsphäre steige mit jeder Weiterverbreitung „seiner" Daten[5]. Dies gilt auch, wenn die Daten auf 1000 Computer in derselben Organisation überspielt oder an 1000 Organisationen oder an ein Drittland mit einer anderen Rechtsordnung weitergegeben werden. Sobald der Einzelne den Besitz an seinen Daten verliert, kann er diesen Prozess nicht aufhalten, es sei denn, die Daten stellen beispielsweise „geistiges Eigentum" dar. In diesem Fall wäre für eine Reproduktion der Daten eine Genehmigung in Form einer Lizenz erforderlich. Wir alle gestalten unser Leben selbst, und es erscheint zunehmend paradox, dass Internetkonzerne Anspruch auf das Eigentum an den Datenmustern erheben, indem sie unser Denken und Verhalten minutiös aufzeichnen, jedoch die Menschen, die diese Daten produzieren, bitten, ihre Autonomie aufzugeben und auf den Schutz ihrer Privatsphäre zu vertrauen.

Der EU-Datenschutzrahmen ist theoretisch deutlich besser als die US-Vorschriften zur Privatsphäre, doch praktisch lassen sich tatsächlich kaum Internetanbieter finden, die Datenschutzgrundsätze benutzerfreundlich und sicher anwenden, indem sie Dienste mit „eingebautem" Datenschutz bereitstellen.

Weltweit haben sich die Regelungen zur Wahrung der Privatsphäre in Anlehnung an zwei konkurrierende Modelle entwickelt. Europa hat einige Rechte des Einzelnen für unveräußerlich erklärt und den mit dem Datenschutz beauftragten Stellen bestimmte Verantwortlichkeiten zugewiesen, während US-Unternehmen die Allgemeinen Geschäftsbedingungen[6] ihrer Nutzungsverträge um Verzichtserklärungen erweitert haben, die eine umfassende Verwendung der Daten erlauben (bekannt als Grundsatz der Informationspflicht und Wahlmöglichkeit).

Die PRISM-Krise entstand unmittelbar im Gefolge der sich seit zehn Jahren herausbildenden Vormachtstellung „kostenloser" Dienste, die aus geografisch entfernten, mit einer Vielzahl von Servern ausgestatteten Rechenzentren von überwiegend der US-Gerichtsbarkeit unterliegenden Unternehmen betrieben werden und als Cloud Computing bekannt geworden sind. Zur Erläuterung dieser Beziehung müssen wir den US-amerikanischen Rechtsrahmen für die innere Sicherheit im Detail beleuchten.

Aufbau und Geltungsbereich

Es fällt auf, dass die europäischen Medien, seit es im vergangenen Jahrzehnt zu ersten Meldungen über „Abhöraktionen ohne richterliche Anordnung" kam, und bis vor recht kurzer Zeit, als die Existenz des Programms PRISM enthüllt wurde, die Kontroversen um die Überwachungstätigkeit der USA als rein doktrinäre Auseinandersetzung über die Bürgerrechte in den USA behandelten und dabei offenbar verkannten, dass diese Tätigkeit **auf den Rest der Welt gerichtet war**.

In diesem Papier soll dieser unterbewertete Aspekt dokumentiert werden. Dabei wird aufgezeigt, dass **der Umfang der Überwachung im Zuge der 2008 vorgenommenen Änderungen des FISA-Gesetzes über das Abhören des Kommunikationsverkehrs hinaus auf alle im öffentlichen Cloud Computing verfügbaren Daten ausgeweitet wurde. Dies hat weit reichende Folgen für die weitere Hoheit der EU über ihre Daten und den Schutz der Rechte ihrer Bürger.** An dieser Stelle soll anhand historischer, technischer und politischer Analysen ein Einblick darin vermittelt werden, wie sich die Überwachung des Internet-Kommunikationsverkehrs durch die US-Regierung

[5] Hondius, Frits W. (1975), Emerging data protection in Europe. North-Holland Pub. Co.
[6] Siehe Dokumentarfilm „Terms and Conditions May Apply" (2013, USA), Regie: Cullen Holback.

entwickelt hat und wie sie das Menschenrecht auf den Schutz der Privatsphäre aus der Sicht des einzelnen EU-Bürgers beeinträchtigt[7]. Gegenstand der Darstellung sind daher:

- I) ein Abriss zur Geschichte der Überwachungstätigkeit der USA im Ausland und derzeit bekannter Stand

- II) ein Überblick über die wichtigsten rechtlichen Kontroversen sowohl in Bezug auf die USA als auch hinsichtlich der Auswirkungen und Folgen für die Rechte der EU-Bürger

- III) Strategieoptionen für das Europäische Parlament und entsprechende Empfehlungen

[7] Während der Abfassung dieses Papiers gab es immer wieder neue, auf dem Material von Snowden beruhende Meldungen. Zwar wurde großer Wert auf Genauigkeit gelegt, doch könnte sich die angebotene Interpretation durch weitere Enthüllungen ändern.

1. GESCHICHTLICHER HINTERGRUND DER ÜBERWACHUNGSTÄTIGKEIT DER USA

WICHTIGSTE ERKENNTNISSE

- Ein Blick auf die Geschichte verschiedener Überwachungsprogramme der USA (Vorläufer von Echelon, PRISM usw.) und der US-Rechtsvorschriften zur Überwachung (FISA und FAA) lässt erkennen, dass die **USA die Grundrechte von Nicht-US-Bürgern durchgängig missachtet haben**.
- Insbesondere entsteht durch den Geltungsbereich des FAA, verbunden mit einer ausdrücklich „politischen" Definition des Begriffs „*ausländische Geheimdienstinformationen*" **eine Befugnis zur gezielten Massenüberwachung der Daten von Nicht-US-Personen**, die sich außerhalb der USA aufhalten; eine Befugnis, die sich der wirksamen Kontrolle im Rahmen von geltenden und geplanten EU-Rechtsvorschriften zum Datenschutz entzieht.

Eine geschichtliche Betrachtung der US-Überwachungsprogramme bietet den Hintergrund für ihre Interpretation als jüngste Phase in einem System, in dem die USA eine Sonderstellung für sich beanspruchen und das seinen Ursprung im Zweiten Weltkrieg nahm. Diese Programme stellen die größte aktuelle Herausforderungen für den Datenschutz dar, da sie willkürlich diskriminierende, streng nach Staatsangehörigkeit und geopolitischen Bündnissen verfahrende Behandlungsmaßstäbe vorsehen, die geheim und mit der Rechtsstaatlichkeit der EU-Strukturen unvereinbar sind.

1.1. Der Zweite Weltkrieg und der Ursprung der UKUSA-Verträge

In den 70er Jahren des 19. Jahrhunderts wurde erstmals das Ausmaß des Erfolgs der Alliierten bei der Kryptoanalyse im Zweiten Weltkrieg bekannt. Die Welt entdeckte die geheime Geschichte von Bletchley Park (auch als Station X bezeichnet), Churchills Zentrale für Fernmelde- und elektronische Aufklärung. Die Geschichte geheimer internationaler Aufklärungspartnerschaften nach dem Krieg ist eng verknüpft mit dem persönlichen Werdegang von Alan Turing, dem bedeutenden Mathematiker und Mitbegründer der Informatik, der entscheidend zur Konstruktion automatisierter Maschinen beitrug, die maschinell generierte Chiffren wie (das für einen Großteil des Nachrichtenverkehrs Nazi-Deutschlands genutzte) Enigma leicht entziffern konnten.

1942 reiste Alan Turing in die USA, um im Auftrag der US-Marine die Massenproduktion von Entzifferungsmaschinen (sogenannten „Bomben") für den Atlantikkrieg zu beaufsichtigen und in den Labors des Bell-Konzerns die Arbeiten an einem neuen Telefon zur Sprachverschleierung („Scrambler") zu überprüfen, das für die Kommunikation zwischen Regierungschefs bestimmt war. Leider verfügte Turing nicht über schriftliche Vollmachten und wurde daher von den US-Einwanderungsbehörden als verdächtig festgehalten, bis ihn Beamte des Vereinigten Königreichs in New York aus dieser Lage befreiten. Aus einer ursprünglich zweiwöchigen Reise wurde ein monatelanger Aufenthalt, da es keinen Präzedenzfall dafür gab, selbst einem ausländischen Verbündeten eine Sicherheitsfreigabe für die Labors zu erteilen, die er besuchen sollte. Die folgenden Monate waren geprägt vom diplomatischen Ringen des Vereinigten Königreichs und Grabenkämpfen zwischen der Marine und dem Heer der USA, da Letzteres keinen Bedarf an der Kenntnis von Ultra (Bezeichnung der aus der Entzifferung in Bletchley gewonnenen Aufklärungsinformationen) hatte. Das Vereinigte Königreich wollte dieses Geheimnis mit möglichst wenigen Menschen teilen, sodass innerhalb der Sicherheitshierarchie des US-Militärs eine Disharmonie entstand, die als „Affäre Turing" bekannt wurde.

Daraus entwickelte sich die geheimdienstliche Partnerschaft der Nachkriegszeit zwischen den USA und dem Vereinigten Königreich als „primären“ Parteien, Kanada, Australien und Neuseeland als „sekundären“ Parteien und anderen Staaten mit geringerer Einsicht in die Informationen als „tertiären“ Parteien. Die entsprechenden Verträge werden als UKUSA-Verträge bezeichnet, und wir kennen die Einzelheiten ihrer Entstehung, da die NSA im Jahr 2010 ihren unredigierten Wortlaut[8] bis zu den 1950er Jahren mit der dazugehörigen Korrespondenz freigab (der aktuelle Text ist Verschlusssache). Demgegenüber gab das GCHQ[9] nicht allzu viel frei, obwohl dieser Schritt als gemeinsame Maßnahme beider Stellen bezeichnet wurde.

Der Zweck der UKUSA-Verträge bestand darin,**abgegrenzte Bereiche der technischen Zusammenarbeit festzulegen und Konflikte zu vermeiden. Allerdings enthalten die für die Jahre bis 1956 veröffentlichten Fassungen keine allgemeine „Antispionageklausel“, sondern Freundschaftsbekundungen, wie sie sich auch in öffentlichen Verträgen finden**. Über die Existenz eines umfassenden Anti-Spionage-Geheimabkommens zwischen dem Vereinigten Königreich und den USA ist nichts bekannt, und keine der beiden Seiten hat jemals über die Legislative oder Exekutive etwas dazu verlauten lassen.

1.2. ECHELON: das Kommunikationsüberwachungsnetz der UKUSA-Allianz

Seit der Gründung der US-amerikanischen Sicherheitsagentur NSA im Jahr 1952 und während des gesamten Kalten Krieges weiteten sowohl das Vereinigte Königreich als auch die USA ihre technischen Kapazitäten für die Fernmelde- und elektronische Aufklärung stark aus, indem sie Seekabel an Landungsstellen anzapften[10], per Satellit terrestrische Richtfunkstrecken abfingen und Antennenanlagen einrichteten, in der Regel in Militärbasen und Botschaften. Die Darstellung der Entwicklung und Beschaffenheit dieser technischen Kapazitäten stützt sich auf zwei quelloffen verfügbare Berichte[11] an die europäischen Organe, die schließlich im Jahr 2000 zur Untersuchung von ECHELON durch das Europäische Parlament führten. ECHELON war ursprünglich ein Deckname für ein spezielles Überwachungssystem, wird jedoch heute im allgemeinen Sprachgebrauch gleichbedeutend für das gesamte Kommunikationsüberwachungsnetz der UKUSA-Allianz verwendet. Die letzte Sitzung des EP-Untersuchungsausschusses fand am 10. September 2001 statt. Der Ausschuss empfahl dem Europäischen Parlament, dass**die Bürger der EU-Mitgliedstaaten bei ihrem Kommunikationsverkehr auf Verschlüsselung zurückgreifen sollten, um ihre Privatsphäre zu schützen**, da die US-Nachrichtendienste offensichtlich Wirtschaftsspionage mit ECHELON betrieben hätten.

[8] Freigabe der UKUSA-Vereinbarung 1940-1956 Early Papers Concerning US-UK Agreement – 1940–1944, NSA/CSS.

[9] Government Communications Headquarters, eine britische Regierungsbehörde, die aus Bletchley Park hervorging und sich mit der Überwachung der inneren Sicherheit durch Kryptologie und nachrichtendienstliche Aufklärung befasst.

[10] Diese Praxis begann im 19. Jahrhundert mit den ersten Telegrafenkabeln und war ein wesentlicher Aspekt der Affäre um die Zimmermann-Depesche, die entscheidend dazu beitrug, die USA zum Eintritt in den Ersten Weltkrieg zu bewegen. Siehe Desai, Anuj C. (2007), , Stanford Law Review, 60 STAN L. REV. 553 (2007).

[11] STOA interception Capabilities (2000) und EuroParl ECHELON (2001) – Berichte von Duncan Campbell.

1.3. 1975-1978: Watergate und der Church-Ausschuss

Nach den Erschütterungen in den USA durch den Watergate-Skandal, der schließlich zum Rücktritt von Richard Nixon führte, richtete der US-Kongress einen Sonderausschuss unter Leitung des Senators Frank Church mit dem Auftrag ein, Amtsmissbrauch durch Strafverfolgungsbehörden und Nachrichtendienste zu untersuchen, die mit Zustimmung des Präsidenten führende Persönlichkeiten aus der inländischen Politik und Zivilgesellschaft illegal abgehört und damit gegen den 4. Zusatzartikel zur US-Verfassung hatten, der das Recht auf Privatsphäre vor willkürlicher Durchsuchung ohne eine richterliche Anordnung schützt, die bei Vorliegen eines „hinreichenden Verdachts" (d. h. bei Indizien für kriminelle Aktivitäten mit einer Wahrscheinlichkeit von 50 %) für diesen Zweck ausgestellt wird.

Der Church-Ausschuss berichtete über die Frage, ob der 4. Zusatzartikel die massive Ausspähung und Sammlung internationaler Kommunikationsdaten einschränkt, die seinen Ermittlungen zufolge seit den 1940er Jahren – anfangs mit Telegrammen – insgeheim durchgeführt worden waren[12]. Der Ausschuss gelangte zu der Feststellung, dass **die unbeabsichtigte Sammlung international übertragener Daten amerikanischer Bürger hinnehmbar sei**, wenn Verfahren zur „Minimierung" von irrtümlichen unberechtigten Zugriffe (und Fehlern, die nicht zum Schaden amerikanischer Bürger begangen wurden) bestünden.

Festgeschrieben wurde dieses Konzept im ersten **Gesetz über die Überwachung der Auslandsgeheimdienste von 1978 (FISA)**, das das Abhören internationaler (und aus dem Inland stammender) „ausländischer Geheimdienstinformationen" von Telekommunikationsunternehmen regelte. Die Sammlung von Daten durch einen Staat außerhalb seines Hoheitsgebiets ist buchstäblich „gesetzlos" und wird in internationalen Übereinkommen nicht ausdrücklich eingeschränkt.

1.4. Im Kontext des 11. September 2001: Ausweitung der Aufklärungsbefugnisse

Nach den Terroranschlägen vom 11. September 2001 wurden die Privatsphäre und der Datenschutz durch außergewöhnliche, im Namen der Sicherheit und des Kampfes gegen den Terrorismus ergriffene Maßnahmen stark beeinträchtigt.

Der **USA PATRIOT Act von 2001** wurde vom US-Kongress am 26. Oktober 2001 erlassen und brachte in erster Linie eine erhebliche Ausweitung der Befugnisse der Strafverfolgungsbehörden zum Sammeln inländischer Geheimdienstinformationen innerhalb der USA mit sich. Der überarbeitete **Foreign Intelligence Surveillance Amendment Act von 2008 (FAA)**[13] sah die Befugnis zur Massenüberwachung speziell von Daten außerhalb der USA befindlicher Nicht-US-Personen vor. Auf diese Aspekte und ihre Folgen für EU-Bürger wird im folgenden Abschnitt (Abschnitt 2) eingegangen.

NSA-Direktor General Hayden schlug Präsident Bush zahlreiche weitere neue Überwachungsprogramme und -modalitäten vor, für die keine ausdrückliche gesetzliche Grundlage bestand, und dennoch wurde die Genehmigung erteilt. Diese Programme wurden rückwirkend in geheimen Memoranden für rechtmäßig erklärt, für deren Ausarbeitung ein

[12] Für die Ausspähung im Rahmen des Programms SHAMROCK (oder des Schwesterprojekts MINARET) bestand keine formale Ermächtigung, doch wurde auf Ersuchen der Regierung täglich ein Magnetband mit der Aufzeichnung aller Telegramme per Kurier an die NSA geliefert. Siehe Snider, Britt L. (1999): Unlucky SHAMROCK – Recollections from the Church Committee's Investigation of NSA.

[13] US-Kongress (2008), Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 122 Stat. 2436, Public Law 110-261, 10. Juli 2008.

relativ niedrig gestellter Rechtsreferent[14] im Rahmen der Genehmigung des Einsatzes militärischer Gewalt (AUMF) im Krieg in Afghanistan und damit verbundene Einsätze im „Krieg gegen den Terror“ zuständig war.

Eines dieser Programme mit dem Decknamen *Stellar Wind* beinhaltete das Anbringen von Kabelteilern („Splitters“) an Glasfaserkabeln in großen Internet-Schaltzentralen und die Echtzeit-Sichtung des enormen Verkehrsaufkommens mit einem kleinen Hochleistungs-Scancomputer (zur Sichtung von Datenpaketen nach dem „Deep-Packet-Inspection“-Prinzip), der derart gefilterte Daten an die NSA zurückleiten sollte. Eine verantwortlicher Techniker vom AT&T-Büro in San Francisco wurde um Mithilfe beim Bau einer solchen Anlage („Room 641A“) gebeten, hatte jedoch die Sorge, dass diese Aktivität offenkundig gegen in der US-Verfassung vorgesehene Schutzmechanismen verstieß, da das Kabel inländische wie internationale Verbindungsdaten transportierte. Er wandte sich mit seiner Geschichte und entsprechendem Beweismaterial an die *New York Times*, die sie ein Jahr lang zurückhielt und erst 2005, nach der Wiederwahl von Präsident Bush, veröffentlichte[15] .

Andere Hinweisgeber von der NSA, dem CIA und dem FBI traten mit Berichten über eine illegale Massenüberwachung per Mobiltelefon, Internet und Satellit an die Öffentlichkeit und enthüllten, dass sogar Telefonate von Barack Obama[16] (damals Senator) und Richtern des Obersten Gerichtshofs abgehört worden seien. Die Kontroverse spitzte sich zu, da zwei Jahre zuvor ein ehemaliger Nationaler Sicherheitsberater[17] ein Forschungsprogramm für *Totale Informationswahrnehmung* (Total Information Awareness, T.I.A.) angeregt hatte, ein System zur Massenüberwachung aller digitalen Daten, die mit fortgeschrittenen Algorithmen auf der Basis künstlicher Intelligenz verarbeitet werden, um geplante Terroranschläge aufzudecken. Aufgrund des sofort einsetzenden negativen Medienechos sah sich der US-Kongress veranlasst, der T.I.A.-Forschung die finanzielle Förderung zu entziehen, doch hielten sich hartnäckige Gerüchte, dass sie in ein sogenanntes „black budget“, ein Geheimbudget, für Aufklärungszwecke geflossen sei.

Als die Behauptungen über „Abhöraktionen ohne richterliche Anordnung“ in einer Reihe von Pressemeldungen der *New York Times*, der *Los Angeles Times* und des *Wall Street Journal* ans Tageslicht kamen, nahm die Besorgnis in der Öffentlichkeit aufgrund des inhaltlichen Zusammenhangs mit dem angeblich eingestellten Projekt T.I.A zu.

1.5. Die Enthüllungen Edward Snowdens und PRISM

Am 5. Juni veröffentlichten die *Washington Post* und der*Guardian* einen nach Abschnitt 215 des PATRIOT Act erlassenen Geheimbefehl, in dem von der Telefongesellschaft Verizon verlangt wurde, der NSA Einzelheiten zu allen innerhalb der USA getätigten und internationalen Telefongespräche zur Verfügung zu stellen, und zwar „laufend“. Am 6. Juni enthüllten die beiden Zeitungen die Existenz eines NSA-Programms mit dem Decknamen PRISM, das auf Daten führender Internetkonzerne der USA zugriff. Noch am selben Tag bestätigte Admiral Clapper (NSA-Direktor) offiziell, dass PRISM bestehe und sich auf Befugnisse nach Abschnitt 702 (oder Paragraf 1881a) des FAA von 2008 stütze. Am 9. Juni gab Edward Snowden in einem Videointerview freiwillig seine Identität preis.

[14] John Yoo, der inoffiziell ebenso verlauten ließ, dass das sogenannte „Waterboarding“ keine Folter darstelle und somit zulässig sei.
[15] *New York Times,* Bush Lets U.S. Spy on Callers Without Courts, *Risen J, Lichtblau E, 16. Dezember 2005.*
[16] *Huffington Post,* Russ Tice, Bush-Era Whistleblower, Claims NSA Ordered Wiretap Of Barack Obama In 2004, *20. Juni 2013.*
[17] Admiral John Poindexter; wurde in den 80er Jahren im Zusammenhang mit der Iran-Contra-Affäre verurteilt und von Präsident Reagan begnadigt.

Die Geschichte wurde zuerst von drei Zeitungen öffentlich gemacht: *The Guardian*, *The Washington Post* und *Der Spiegel*. Bei der Beschaffung und Analyse des Materials und seiner Auslegung für die Allgemeinheit haben vier Journalisten eine maßgebliche Rolle gespielt: Barton Gellman, Laura Poitras, Jacob Appelbaum und Glenn Greenwald. Daran beteiligt waren auch die US-Ausgabe des *Guardian* und die *New York Times* in Partnerschaft mit *ProPublica*, nachdem die britische Regierung darauf gedrängt hatte, dass der *Guardian* die in seinem Londoner Büro befindliche Kopie des Snowden-Materials unter Aufsicht des GCHQ vernichtet[18].

Im sogenannten „PRISM-Skandal" wurde eine Reihe von Überwachungsprogrammen aufgedeckt, darunter:

1.5.1 „Upstream"

Die veröffentlichten Folien aus dem Snowden-Fundus enthalten Verweise auf NSA-Programme zur Datensammlung im Rahmen von „Upstream", was durch mehrere Decknamen angedeutet wird. Dabei werden Daten öffentlicher wie privater Netze von Landungsstellen transatlantischer Glasfaserkabel und von Schaltzentralen, die den Internetverkehr zwischen den großen Anbietern lenken, auf der Grundlage von Vereinbarungen mit den Betreibern oder an sie ergangene richterliche Anordnungen (und wahrscheinlich bei Bedarf auch durch das Anzapfen von Kabeln auf dem Meeresboden[19]) abgezweigt und in Kopie an die NSA geleitet.

1.5.2 XKeyscore

Das System XKeyscore wurde in Folien[20] (von 2008[21]) beschrieben, die am 31. Julivom *Guardian* veröffentlicht wurden. Es handelt sich dabei um ein „System zur Ausnutzung/Analyse digitaler Informationen", das eine Durchsuchung „ungefilterter Daten" im „durchlaufenden Pufferspeicher im Rhythmus von drei Tagen" ermöglicht, die an 150 globalen Standorten auf 700 Servern gespeichert sind. In dem System werden Daten zusammengeführt, die von US-Botschaftsstandorten, ausländischen Satelliten- und Richtfunkübertragungen (d. h. dem früher als ECHELON bekannten System) und aus den oben genannten Quellen des Programms „Upstream" stammen[22] .

Das System bietet eine Indexierung nach E-Mail-Adressen, Dateinamen, IP-Adressen und Portnummern, Cookies, Nutzernamen für Webmail- und Chatfunktionen und Freundeskreis-Listen, Telefonnummern und Metadaten aus Surfsitzungen (darunter in Suchmaschinen eingegebene Wörter und in Google Maps aufgerufene Orte). Der entscheidende Vorteil des Systems besteht darin, dass es einem Analysten erlaubt, „starke Selektoren" (Suchparameter, die ein Ziel identifizieren oder die Extraktion von Daten genau zu diesem Ziel ermöglichen) anzuwenden und nach „abweichenden Ereignissen" zu suchen, z. B. nach jemandem, der „Verschlüsselungstechnik nutzt" oder „nach verdächtigen Inhalten sucht".

Der Analyst kann die Ergebnisse dieser Indexsuchen nutzen, um „Inhalte vom jeweiligen Standort nach Bedarf einfach herüberzuholen". Mit diesem vereinheitlichten Suchsystem

[18] Eine vollständige Analyse der Enthüllungen würde den Rahmen dieses Berichts sprengen, doch wird bei der folgenden Darstellung von der Echtheit der Powerpoint-Folien und der Dokumente ausgegangen. Ernst zu nehmende gegenteilige Behauptungen wurden bislang nicht vorgebracht.

[19] Auf die Existenz US-amerikanischer U-Boote, die eigens für das Anzapfen von Unterseekabeln ausgerüstet sind, wurde in dem Bericht des EP von 2000 zu ECHELON hingewiesen; siehe „Ivy Bells".

[20] http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-programme-full-presentation

[21] Im Juli 2013 erschien eine Stellenanzeige eines Rüstungsunternehmens, die andeutete, dass das Programm noch laufe.

[22] http://theweek.com/article/index/247684/whats-xkeyscore

lassen sich rückwirkend für drei Tage (Stand: 2008) Datenmengen erfassen, die wesentlich höher sind als das für eine Rückleitung an die NSA machbare Maß.

Das System ist ebenso zur personalisierten Datensammlung in der Lage, d. h., ein „abweichendes Ereignis" kann als potenzielles Merkmal einer bestimmten Zielperson auch ohne Kenntnis eines „starken Selektors" eine Sammlung von Daten zu dieser Person auslösen. Ferner ist es möglich, „alle angreifbaren Rechner in Land X" zu finden, indem der „Fingerabdruck" der in den erfassten Datenströmen angezeigten Konfigurationen mit der NSA-Datenbank für bekannte Software-Schwächen abgeglichen wird. Darüber hinaus kann den Folien zufolge auch nach allen Excel-Tabellen mit „MAC-Adressen aus Irak" gesucht werden[23].

Folie 17 ist insofern bemerkenswert, als sie die ersten Anzeichen für eine systematische Angreifbarkeit von Verschlüsselungssystemen enthält[24] (siehe BULLRUN unten).

1.5.3 BULLRUN

BULLRUN[25] ist der Deckname eines von der NSA in den vergangenen zehn Jahren betriebenen Programms mit dem Ziel, „durch aggressive und mehrgleisige Anstrengungen weithin verwendete Verschlüsselungstechnologien zu brechen", wie aus einer am 1. September vom *Guardian*[26]und der*New York Times* gemeinsam veröffentlichten Meldung hervorging. Dieses Programm hat mehr als alle anderen bisherigen Erkenntnisse aus dem Snowden-Material für Bestürzung unter Experten für Internetsicherheit gesorgt. Weltweit bemüht man sich verzweifelt, abzuschätzen, welche Systeme angreifbar sein könnten, und Schlüssel, Chiffren und Systeme zu verbessern oder zu ändern, nicht zuletzt weil Angreifer aus feindlich gesinnten Ländern nun versuchen werden, bislang nur der NSA bekannte „Hintertüren" für sich zu entdecken.

In dem mit einem Jahresetat von 250 Mio. USD ausgestatteten Programm kommen vermutlich einige der folgenden Methoden zum Einsatz: Zusammenarbeit mit Anbietern von IT-Sicherheitsprodukten und entsprechender Software, mathematische Kryptoanalyse und „Seitenkanalattacken", die Fälschung digitaler Zertifikate, die Unterwanderung und Beeinflussung technischer Gremien im Hinblick auf die Annahme unsicherer Standards und wahrscheinlich der Einsatz richterlicher Zwangsanordnungen mit dem Ziel, den Einbau von „Hintertüren" zu forcieren. Es ist wichtig, zu betonen, dass (noch) keine Beweise dafür zutage getreten sind, dass die allgemein verwendeten grundlegenden Chiffrieralgorithmen mathematisch gebrochen wurden, doch nimmt seit einigen Jahren die Sorge über mögliche Schwachstellen in komplexen „Protokollen" für die Einrichtung und Gewährleistung der Kompatibilität zwischen den gängigen Softwareprogrammen zu.

[23] Dies mutet ungewöhnlich an, da Microsoft angeblich seit Office 2000 die MAC-Adresse nicht mehr zum Bestandteil des GUID (Global Unique Identifier, dient zur Erzeugung einer global eindeutigen Dokumentenindexnummer) macht und MAC-Adressen keinem bestimmten Land zugeordnet werden können (es sei denn, die NSA hat sich irgendwie eine umfassende Datenbank beschafft oder eine solche speziell für Irak angelegt oder ist in der Lage, WiFi-Signale auf große Entfernung und/oder systematisch zu überwachen und abzufangen).

[24] „Zeige mir alle VPN-Anbieter in Land X und gib mir die Daten, damit ich die Nutzer entschlüsseln und ausfindig machen kann" – ein VPN (Virtual Private Network, virtuelles privates Netz) ist ein „verschlüsselter Tunnel" zwischen dem Computer des Nutzers und einem VPN-Anbieter und erweckt im Interesse der Privatsphäre des Nutzers und aus Sicherheitsgründen den Anschein, dass der Internetverkehr nicht von ihm, sondern vom VPN-Anbieter stammt.

[25] Unter dem entsprechenden Decknamen EDGEHILL betreibt GCHQ ein ähnliches Programm für das Eindringen in verschlüsselte Systeme, das kurioserweise ebenso wie BULLRUN nach einer Bürgerkriegsschlacht des Landes benannt wurde, allerdings nicht Gegenstand dieses Papiers ist.

[26] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Nach FISA Abschnitt 702 können Diensteanbieter *„zur unverzüglichen Bereitstellung aller erforderlichen Informationen, Anlagen oder Hilfen an die Regierung für den Erwerb“* ausländischer Geheimdienstinformationen angehalten und damit an sich zur Offenlegung kryptografischer Schlüssel gezwungen werden, wozu auch SSL-Schlüssel für die Sicherung von Daten bei der Übertragung durch große Suchmaschinen, soziale Netzwerke, Webmail-Portale und Cloud-Dienste allgemein gehören. Es ist noch nicht bekannt, ob diese Befugnis bislang eingesetzt wurde.

2. NSA-PROGRAMME UND DAMIT VERBUNDENE RECHTSVORSCHRIFTEN: KONTROVERSEN, LÜCKEN UND SCHLUPFLÖCHER SOWIE FOLGEN FÜR EU-BÜRGER

WICHTIGSTE ERKENNTNISSE

- Aufgrund des komplexen Beziehungsgeflechts zwischen den US-Rechtsvorschriften zu „geheimdienstlichen Informationen" und ihrer Auslegung durch geheime Gerichte und Rechtsmemoranden der Exekutive haben sich rechtswidrige Praktiken herausgebildet, die **sowohl US-Bürger als auch Nicht-US-Bürger betreffen**.
- Aus dieser Rechtsunsicherheit und dem fehlenden Schutz von Nicht-US-Bürgern durch den 4. Zusatzartikel ergibt sich, dass **Nichtamerikaner** gegenüber den US-Behörden nach FISA **keine anerkannten Rechte in Bezug auf die Privatsphäre** besitzen.
- Der dem immer rascher zunehmende und bereits weitverbreitete Einsatz von **Cloud Computing höhlt den Datenschutz für EU-Bürger weiter aus**.
- Eine Bestandsaufnahme der Mechanismen für die Weitergabe von Daten, die in der EU zum Schutz der Rechte von EU-Bürgern geschaffen wurden, zeigt, dass diese **als Schlupflöcher wirken**.

Eine Analyse der bekannten Überwachungsprogramme der USA und der diesbezüglichen Rechtsvorschriften aus grundrechtlicher Sicht ergibt zwei Kategorien rechtlicher „Grauzonen", die in ständiger Wechselwirkung stehen[27]:

- das Fehlen von Rechtssicherheit, das innerhalb der USA zu Eingriffen in die Privatsphäre und anderen potenziellen Missbräuchen und Unregelmäßigkeiten führt, obwohl diese Auswirkungen auf amerikanische Staatsbürger und andere in den USA ansässige Personen angeblich nicht beabsichtigt sind.

- der mit den US-Gesetzen FISA (und PATRIOT Act) verfolgte Zweck, „ausländische Geheimdienstinformationen" über Menschen zu gewinnen, die weder amerikanische Staatsbürger noch in den USA rechtmäßig ansässige Personen sind.

2.1. Rechtliche Lücken und Unsicherheiten in den US-Rechtsvorschriften zum Schutz der Privatsphäre: Folgen für US-Bürger und in den USA ansässige Ausländer

[27] Forgang, Jonathan D., (2009), "The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas, Fordham Law Review, Volume 78, Issue 1, Article 6, 2009.

2.1.1 Die Doktrin der Weitergabe an Dritte und Einschränkungen des 4. Zusatzartikels

Im Zusammenhang mit zwei US-Rechtssachen, 1976 und 1979, wurde eine Rechtsdoktrin geschaffen, wonach bei der Weitergabe personenbezogener Daten an Dritte wie Banken oder Telefongesellschaften, die diesen anvertraut oder von ihnen zur Nutzung einer Dienstleistung angefordert werden, keine berechtigte Erwartung auf Wahrung der Privatsphäre besteht, weshalb kein Durchsuchungsbefehl gemäß dem 4. Zusatzartikel benötigt wird, der das Recht auf Privatsphäre vor willkürlicher Durchsuchung ohne eine richterliche Anordnung schützt, die bei Vorliegen eines „hinreichenden Verdachts" (d. h. bei Indizien für kriminelle Aktivitäten mit einer Wahrscheinlichkeit von 50 %) für diesen Zweck ausgestellt wird. Demzufolge können Strafverfolgungsbehörden auf Geschäftsunterlagen wie Kreditkartentransaktionen, Kontoauszüge und detaillierte Telefonrechnungen mit Einzelverbindungsübersicht zugreifen, indem sie Verwaltungsverfahren anwenden, die von ihnen selbst statt von einem unabhängigen Richter genehmigt wurden, und müssen keinen „hinreichenden Verdacht" nachweisen.

Diese Doktrin war im Zuge der Entwicklung der Mobilfunkkommunikation, die den Standort von Teilnehmern verfolgt, von Internetdiensten, die die Navigation auf Webseiten und die Nutzung von Suchmaschinen aufzeichnen, und von sozialen Netzwerken, die allein durch ihren Aufbau und die Dynamik ihrer sozialen Interaktion intime [28]Details aus dem Privatleben[29]offenbaren, immer wieder Gegenstand der Kritik. Offensichtlich konnten die Gerichte diese Umstände in den 1970er Jahren nicht vorhersehen, doch erwies sich bislang jeder Versuch zur Abschaffung der Doktrin als erfolglos.

Diese Bedenken hinsichtlich des Schutzes der Privatsphäre nahmen mit Abschnitt 215 des USA PATRIOT Act von 2001 zu, der eine erhebliche Kontroverse auslöste. Demnach dürfen sich Sicherheitsbehörden mit geheimer richterlicher Anordnung konkrete Geschäftsunterlagen bei Unternehmen beschaffen. Auch wenn die Möglichkeit geheimer *nicht*-richterlicher Anordnungen zur Beschaffung von „Daten ohne Kommunikationsinhalte" (d. h. Metadaten) bereits nach dem als „National Security Letter" bezeichneten Verfahren (eine im US-Recht vorgesehene Anordnung bei Ermittlungen zur inneren Sicherheit) bestand, gilt Abschnitt 215 für „konkrete" Daten aller Art, die sich im Besitz einer großen Vielfalt von Unternehmen des Privatsektors befinden.

Nach den ersten Enthüllungen über das Programm PRISM bestätigte General Alexander (NSA-Direktor) bei zwei öffentlichen Anhörungen vor den Kongressausschüssen zur Überprüfung der geheimdienstlichen Tätigkeit, dass die NSA Metadaten zu (inländischen wie internationalen) Telefonverbindungen von allen großen Anbietern sammelt und sie fünf Jahre lang in einer entsprechenden Datenbank speichert[30]. Nach eigenen Angaben nutzt die NSA diese Daten allein zur Entscheidung darüber, ob ein „deutlich begründbarer Verdacht" eines Zusammenhangs mit einer Ermittlung wegen Terrorismus besteht. Die Datenbank

[28] Agarwal, A., Rambow, O. & Bhardwaj, N. (2009) Predicting Interests of People on Online Social Networks, CSE 2009: International Conference on Computational Science and Engineering.

[29] Mislove, A., Viswanath, B., Gummadi, K.P. & Druschel, P. You are who you know: inferring user profiles in online social networks, Proceedings of the Third ACM International Conference on Web Search and Data Mining ACM, 2010, S. 251-260.

[30] Die New York Times enthüllte am 1. September unter Berufung auf eine andere Quelle als Snowden, dass die Telefongesellschaft AT&T seit 1987 alle Verbindungsdaten zu Fern- und internationalen Gesprächen speichert und sie der US-Drogenbehörde „Drug Enforcement Agency" im Rahmen eines Geheimprogramms mit dem Decknamen HEMISPHERE für ihre Drogenfahndungen zur Verfügung stellt. In der der EU wäre die Aufbewahrung solcher Daten über die in der Vorratsdaten-Richtlinie von 2006 vorgesehene Höchstdauer von zwei Jahren hinaus nach der Datenschutzrichtlinie für elektronische Kommunikation von 2002 (und der früheren ISDN-Richtlinie von 1998) illegal, da diese vorschreiben, dass die Daten gelöscht oder anonymisiert werden, wenn der rechtmäßige Geschäftszwecke wegfällt.

wird danach durchsucht, ob die Telefonnummer einer Zielperson über „drei Ecken“ mit einem anderen, bereits mit Terrorismus in Zusammenhang gebrachten Netz von Nummern verbunden ist (d. h. ob zu einem bestimmten Zeitpunkt in den letzten fünf Jahren eine „Telefonkette“ bestanden hat).

2.1.2 KDS und „Relevanztest“

Die bislang größte rechtliche Kontroverse in den USA im Zusammenhang mit Snowdens Enthüllungen betrifft eigentlich nicht PRISM, sondern die unterschiedslose, flächendeckende und vom PATRIOT Act offenbar nicht abgedeckte Sammlung aller Telefon-Metadaten in Form von Kommunikationsdatensätzen (KDS). Daten dürfen ohnehin nur dann nach Abschnitt 215 gewonnen werden, wenn sie das Erfordernis erfüllen, für eine genehmigte Ermittlung „relevant“ zu sein. Das Relevanzerfordernis wurde mit der Änderung des PATRIOT Act im Jahr 2006 mit der Absicht eingeführt, die Datensammlung einzuschränken[31], wird allerdings wohl als Rechtfertigung für eine massive Datenabschöpfung interpretiert.

Die Beweggründe für diese Datensammlung sind daher fragwürdig: Wie lässt es sich überhaupt rechtfertigen, dass eine gesamte Datenbank aufgrund der Annahme angelegt wurde, dass die Telefonnummer einer bestimmten Verdachtsperson über „drei Ecken“ eine Verbindung zum Terrorismus aufweist? Ein Interessenanwalt formulierte es prägnant so: *„Sie haben verdachtslose Abfragen durchgeführt, um den Verdacht zu erlangen, den das FISA-Gericht benötigt, damit Abfragen durchgeführt werden können.“*[32]

Die durch das FISA aufgeworfenen Probleme wurden der Auslegung des *Gerichts für die Überwachung der Auslandsgeheimdienste* (FISC) und des ihm übergeordneten Revisionsgerichts (FISCR) (in geheimen Sitzungen) überlassen, deren Richter ausschließlich vom Chefrichter des Obersten Gerichtshofs der USA ernannt werden. Offensichtlich stimmen die FISA-Gerichte dem Argument der Regierung zu, dass bei Ermittlungen üblicherweise ein unendlich großer Fundus von Daten als „relevant“ angesehen wird, um tatsächliche Beweise zu finden. Einige der Geheimgutachten des FISC und des FISCR werden derzeit offiziell freigegeben, haben jedoch diesen logischen Widerspruch bislang nicht erklären können.

2.1.3. „Direkter Zugriff“ auf Datenzentren für Überwachungszwecke?

Die in den PRISM-Folien genannten Unternehmen haben den „direkten Zugriff“ auf ihre Datenzentren, der aus ihren „Marketing-Folien“ ersichtlich war und die Existenz von PRISM offenbarte, sofort dementiert. Sie erklärten, lediglich einem verbindlichen Gerichtsbeschluss gefolgt zu sein und nie von dem Decknamen PRISM gehört zu haben (was nicht überrascht, da die NSA damit ein streng geheimes Programm bezeichnete). Microsoft behauptete, nur auf Anfragen reagiert zu haben, die konkrete Kontoidentifikatoren enthielten, während Google und Facebook bestritten, in ihren Netzwerken „schwarze Kästen“ für den „direkten Zugriff“ installiert zu haben. Den Unternehmen sind durch die Geheimhaltungsbestimmungen von Abschnitt 702 die Hände gebunden, die eine Strafandrohung wegen Missachtung des Gerichts oder gar eine Anklage wegen Spionage

[31] Nach Äußerungen des Kongressabgeordneten Jim Sensenbrenner, Patriot Act Architect Criticizes NSA's Data Collection im Sender NPR am 20. August 2013.

[32] https://www.eff.org/deeplinks/2013/09/government-releases-nsa-surveillance-docs-and-previously-secret-fisa-court

vorsehen[33]. Google und Microsoft führen derzeit Klage gegen die Regierung, um deren Genehmigung für die Veröffentlichung von Einzelheiten zur Zahl der von Anordnungen nach FISA betroffenen Personen zu erstreiten.

Zwischen den sorgfältig und wortgewandt abgefassten (und anscheinend abgestimmten[34]) Dementi der Unternehmen und den Berichten über PRISM besteht jedoch keine sachliche Unstimmigkeit. Die Formulierung „direkter Zugriff" dürfte dazu gedient haben, diese Modalität von der Datensammlung im Rahmen von „Upstream" (siehe oben) abzugrenzen, da sie nicht unbedingt im wörtlichen Sinn nahelegt, dass Daten ohne Wissen des Unternehmens abgeschöpft werden konnten. Ein „direkter Zugriff" dieser Art wird jedoch durch den Abschnitt 702 nicht ausgeschlossen und ist möglicherweise bereits bei anderen Unternehmen vorgekommen oder kann künftig vom FISC gestattet werden.

Eine entscheidende weitere Entwicklung ergab sich aus einer in der*New York Times*[35] vom 8. August geäußerten aufmerksamen Beobachtung, dass „Selektoren", die in den am 20. Juni offengelegten Verfahren zur Auswahl von Zielpersonen verwendet werden, um die Informationen für einen Zugriff nach Abschnitt 702 genauer zu bestimmen, auch willkürliche Suchbegriffe umfassen könnten. Wenn dies vom reinen Wortlaut des Gesetzes her auch keine Überraschung sein dürfte, wurde dennoch deutlich, dass die Privatsphäre von Amerikanern (und natürlich Nichtamerikanern) willkürlichen Abfragen großer Datenmengen unterliegt und der Zugriff nicht auf Kontoidentifikatoren beschränkt ist, die mit einer Wahrscheinlichkeit von 50 % als nichtamerikanisch eingeschätzt werden. In einem weiteren Bericht trat zutage[36], dass das FISA-Gericht 2011 auf Ersuchen der Regierung ein früheres Urteil aufhob und fortan die Verwendung willkürlicher Suchbegriffe gestattete, **selbst wenn** sie für Amerikaner kennzeichnende Faktoren für die Zielauswahl einschlossen.

Offenkundig wurden also die im Gesetz allein für Amerikaner vorgesehenen theoretischen Schutzvorkehrungen durch immer weit reichendere Ersuchen der Regierung an das Gericht stark untergraben[37].

2.1.4 Die Geheimbudgets der Nachrichtendienste: Umfang und Kosten der US-Kapazitäten

Am 31. August veröffentlichte die*Washington Post* Einzelheiten zum geheimen („schwarzen") Budget[38] der Geheimdienstgemeinschaft der USA, das sich auf jährlich 50 Mrd. USD beläuft, und eine Aufschlüsselung der Ausgaben nach mehreren Kategorien. Den Meldungen zufolge hatten die USA seit dem 11. September 2001 500 Mrd. USD für die geheime Aufklärung aufgewandt. Der Jahresetat der NSA beträgt etwa 10 Mrd. USD, doch zeigten sich die Kommentatoren überrascht, dass der Haushalt des CIA rasch auf 15 Mrd. USD angestiegen ist und damit den der NSA übersteigt.

[33] http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance

[34] Die Erklärungen von Google und Facebook weisen im Wortlaut zahlreiche Übereinstimmungen auf, was stark auf einen gemeinsamen Ursprungstext hindeutet.

[35] .http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=1&hp

[36] .http://www.washingtonpost.com/politics/federal_government/report-surveillance-court-ruling-allowed-nsa-search-of-domestic-email/2013/09/08/4d9c8bb8-18c0-11e3-80ac-96205cacb45a_story.html

[37] Cloud, Morgan (2005), A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment, Ohio State Journal of Criminal Law, Vol 3:33 2005.

[38] .http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

2.2. Die Lage von Nicht-US-Bürgern und nicht in den USA ansässigen Personen (Nicht-US-Personen)

Im bisherigen Verlauf der „Snowden-Affäre“ fällt auf, dass die innenpolitische Berichterstattung in den USA nahezu ausschließlich die Rechte von*Amerikanern*erwähnt. Das ist nicht als rhetorische Figur, sondern wörtlich zu verstehen -– es sollte nicht von einer Gegenseitigkeit [39] (im Gesetz oder im öffentlichen Diskurs) ausgegangen werden, die den Geltungsbereich der Rechte ausweitet[40]. Die Rechte von Nichtamerikanern finden in den US-Medien [41] oder den US-Rechtsvorschriften kaum Erwähnung. Noch erstaunlicher ist, dass – wie aus einer sorgfältigen Analyse der Bestimmungen von Abschnitt 702 des FISA-Gesetzes eindeutig hervorgeht – zwei verschiedene Systeme für die Verarbeitung und den Schutz der Daten bestehen: eines für US-Bürger und in den USA ansässige Personen („US-Personen“), ein weiteres für Nicht-US-Bürger und nicht in den USA ansässige Personen („Nicht-US-Personen“), das ihnen keinerlei Schutz bietet.

2.2.1 Politische Definitionen „ausländischer Geheimdienstinformationen“

Die FISA-Definition „ausländischer Geheimdienstinformationen“ wurde mehrmals geändert und um spezifische und eindeutige Kategorien erweitert, etwa Geldwäsche, Terrorismus und Massenvernichtungswaffen, enthält jedoch schon immer zwei Elemente mit nahezu unbegrenztem Geltungsumfang. Vereinfacht ausgedrückt umfasst sie[42]:

> *Informationen über eine im Ausland ansässige politische Organisation **oder** ein ausländisches Hoheitsgebiet, die sich aufdie Durchführung der Außenpolitik der USA **beziehen** und, sofern sie eine **US-Person** betreffen, dafür**erforderlich** sind. [Hervorh. d. Verf.]*

In Anbetracht einer derart generischen Definition stellt es sich für einen Nichtamerikaner so dar:**Alle für die US-Außenpolitik hilfreichen Daten kommen in Betracht, auch ausdrücklich die politische Überwachung gewöhnlicher und rechtmäßiger demokratischer Aktivitäten**.

2.2.2. Besondere Befugnisse über den Kommunikationsverkehr von Nicht-US-Personen

Um der öffentlichen Kontroverse[43] über das „Abhören“ von Amerikanern „ohne richterliche Anordnung“ ein Ende zu setzen, erließ[44] der US-Kongress 2007 das Interimsgesetz Protect America Act (PAA) zur Änderung des FISA-Gesetzes von 1978 und schuf eine neue Befugnis speziell für den Kommunikationsverkehr von Nicht-US-Personen, die sich außerhalb des US-Hoheitsgebiets befinden (d. h. 95 % der restlichen Weltbevölkerung). Am stärksten

[39]. Corradino, Elizabeth A., (1989), Fordham Law Review, The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far? Volume 57, Issue 4, Article 4, Januar 1989.
[40]. Cole, David, (2003), Georgetown Law: The Scholarly Commons, Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens? 25 T. Jefferson L. Rev. 367-388.
[41].Kenneth Roth (Direktor von Human Rights Watch), 4. September 2013: „... die Rechte von Nichtamerikanern außerhalb der Vereinigten Staaten sind anzuerkennen“.
[42] 50 USC §1801(e)2(B) - http://www.law.cornell.edu/uscode/text/50/1801
[43] Bloom, Stephanie Cooper (2009), What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform, Public Interest Law Journal Vol 18:269.
[44] Congressional Research Service (2007), P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, 23. August 2007.

heizte sich die politische Debatte bei der Frage auf, ob die Telekommunikationsunternehmen durch ihre Kooperation gegen die Rechtsvorschriften zur Privatsphäre ihrer Kunden verstoßen hatten. Je nach der umstrittenen Rechtmäßigkeit des Rückgriffs auf das Konzept der***Genehmigung des Einsatzes militärischer Gewalt*** (**AUMF**) als Auslöser für die Überwachung, die die Rechte von Amerikanern beeinträchtigt hatte, hafteten die Unternehmen potenziell auf Schadensersatz in Milliardenhöhe. Die Telekommunikationsunternehmen und die Internet-Branche bestanden unnachgiebig auf vollständiger zivilrechtlicher Immunität als ihrem Preis für eine künftige Kooperation. Hier ist es der Hinweis unerlässlich, dass es bei dieser Kontroverse um die Folgen für die Privatsphäre von Amerikanern ging und dass die Überwachung von außerhalb der USA lebenden Ausländern über ihren Kommunikationsverkehr in Richtung **oder über** die USA als *unabänderliche Tatsache*und nationales Vorrecht verstanden wurde[45].

2.2.3. Der 4. Zusatzartikel gilt nicht für Nicht-US-Personen außerhalb der USA

Nun kann der Zusammenhang zwischen der Kontroverse über die durch Abschnitt 215 des PATRIOT Act verliehene Befugnis und dem Rückgriff auf die in Abschnitt 702 des FISA-Gesetzes verankerte Befugnis im Programm PRISM erläutert werden. Die Einzelheiten zu Inlands- und Auslandsgesprächen über einen Zeitraum von fünf Jahren umfassende Datenbank wurde dazu genutzt, eine Begründung für die Terrorismusbekämpfung (nach dem Prinzip der Verbindung „über drei Ecken“) zu geben. Anschließend wurde eine zweite Datenbank abgefragt, die ein von der NSA geführtes Verzeichnis von mutmaßlich amerikanischen Telefonnummern enthält. Ergab die Abfrage, dass die Nummer wahrscheinlich nicht die eines Amerikaners war, konnte der Inhalt des Gesprächs gemäß Abschnitt 702 des FISA-Gesetzes ohne weitere Genehmigung abgehört werden. Handelte es sich dagegen wahrscheinlich um die Nummer eines Amerikaners, wäre (gemäß einem anderen Abschnitt von FISA) für das Abhören eine weitere spezifische richterliche Anordnung erforderlich gewesen, um den Eingriff in die Privatsphäre bei deutlich höheren Rechtsauflagen und unter Nennung der Umstände des jeweiligen Falls zu begründen.

Eine gründliche Lektüre von Abschnitt 215 lässt jedoch erkennen, dass ein anderer Zweck (als eine Verbindung zum Terrorismus) darin besteht,*„ausländische Geheimdienstinformationen zu erlangen, die keine US-Person betreffen“*[46]. Aus nichtamerikanischer Sicht mag das als wichtiger, bislang in keiner der in den USA durchgeführten Analysen angesprochener Punkt erscheinen. Ebenso unklar ist, wie diese Bestimmung Licht in die ohnehin schon verworrene Rechtmäßigkeitsdebatte bringen könnte. Sie ist jedoch**ein weiteres anschauliches Beispiel für eine US-Rechtsvorschrift, die zwischen dem durch die Verfassung gewährten Schutz für US-Bürger und allen anderen Personen unterscheidet**.

In einer Reihe aufschlussreicher Interviews betonte der ehemalige NSA-Direktor, General Hayden, dass „*der 4. Zusatzartikel* – der willkürliche Durchsuchungen und Beschlagnahmen untersagt und für einen Haussuchungsbefehl eine richterliche Anordnung und einen hinreichenden Verdacht voraussetzt – *kein internationaler Vertrag* “[47] sei und dass die USA hinsichtlich des ungehinderten Zugriffs auf den ausländischen Kommunikationsverkehr, der über das US-Hoheitsgebiet geleitet wird, oder Auslandsdaten, die dort gespeichert werden, einen „Heimvorteil“ hätten.

[45] Congressional Research Service (2007), P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, August 23, 2007 und Congressional Research Service – Liu, Edward C. (2013), Reauthorization of the FISA Amendments Act, 7-5700, R42725, 2. Januar 2013.
[46] http://www.law.cornell.edu/uscode/text/50/1861
[47] CBS News 30. Juni 2013; eine weitere Diskussion findet sich bei YOUNG (2003), a. a. O.

Diese Äußerungen sind schlecht mit Redebeiträgen und Erklärungen vereinbar, die Beamte des US-Außenministeriums vor 2012 auf Foren wie der Oktopus-Konferenz des Europarats zur Computerkriminalität und der jährlichen Internationalen Konferenz der Datenschutzbeauftragten abgaben und in denen sie den Schutz durch den 4. Zusatzartikel priesen[48]. Da diese Erklärungen an ein internationales Publikum gerichtet waren und die Gewissheit bieten sollten, dass die USA die Privatsphäre achteten, können sie in der Rückschau nur als Täuschung ausgelegt werden[49]. Der Verfasser forderte 2012 einen US-Vertreter öffentlich auf, unmissverständlich zu erklären, dass der 4. Zusatzartikel auch für (außerhalb der USA befindliche) Nicht-US-Personen gelte, erhielt jedoch keine Antwort.

2.2.4. Risiken des Cloud Computing für Nicht-US-Personen

Das oben genannte Interimsgesetz Protect America Act von 2007 sollte kurz vor den Präsidentschaftswahlen von 2008 auslaufen. Sein Geltungsbereich war auf das Abhören der Daten von Telefon- und Internetanbietern beschränkt. Präsidentschaftskandidat Obama stimmte einer fraktionsübergreifenden Einigung zu, das PAA-Gesetz und die darin vorgesehene Immunität für Telekommunikationsunternehmen mit dem im Juli 2008 erlassenen Gesetz zur Änderung von FISA auf eine dauerhafte Grundlage zu stellen.

Das FAA-Gesetz enthielt bei seiner Einführung drei zusätzliche Worte, die anscheinend von niemandem bemerkt und kommentiert wurden[50]. Mit dem Einschub von „remote computing services“ (ausgelagerte Datendienste – ein Begriff aus dem Gesetz über den Schutz der Privatsphäre in der elektronischen Kommunikation (Electronic Communications Privacy Act, ECPA) von 1986, das den Zugriff der *Strafverfolgungsbehörden* auf gespeicherte Verbindungen regelt), **wurde der Geltungsbereich über Internet- und Telefonverbindungen hinaus drastisch ausgeweitet und erfasst nun auch Cloud Computing.**

Cloud Computing kann allgemein als verteilte Datenverarbeitung auf geografisch entfernten Computern definiert werden, auf die über das Internet zugegriffen wird. Seit 2007 wurden die Vorzüge des Cloud Computing für Unternehmen, Regierungen und politische Entscheidungsträger im Marketing der Internetbranche geradezu missionarisch angepriesen, zuerst von Google, rasch gefolgt von Microsoft und anderen Konzernen, was einen neuen Sektor für Unternehmenssoftware entstehen ließ.

2012 beauftragte der LIBE-Ausschuss das*Centre for European Policy Studies* (CEPS) und das *Centre d'Etudes sur les Conflits, Liberté et Securité* (CCLS) mit der Erarbeitung eines Themenpapiers über die Bekämpfung der Computerkriminalität und den Schutz der

[48] Siehe Medina, M. Isabel, (2008) Indiana Law Journal, Exploring the Use of the Word "Citizen" in Writings on the Fourth Amendment Volume 83, Issue 4, Article 14, Januar 2008.

[49] Siehe die Bemerkungen des US-Botschafters bei der EU (2012), Remarks by William E Kennard, auf der am 4. Dezember 2012 vom Forum Europe abgehaltenen dritten jährlichen Europäischen Datenschutzkonferenz, wobei die in Bezug auf das Strafrecht abgegebenen Zusicherungen nicht für das nicht erwähnte FISA-Gesetz gelten, siehe auch: US-Außenministerium (2012), Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the EU and the US.

[50] Eine ausführlichere Darstellung ausgelagerter Datendienste nach dem ECPA-Gesetz findet sich bei: Pell, Stephanie K. (2012), Systematic government access to private-sector data in the United States, International Data Privacy Law, 2012, Vol. 2, No. 4.

Privatsphäre in der Cloud und bat den Verfasser um Mitarbeit[51]. Einige Abschnitte des Papiers enthalten**eindeutige Feststellungen darüber, dass das Cloud Computing und die diesbezüglichen US-Regelungen eine Bedrohung für die Datenhoheit der EU in bislang ungekannten Ausmaß darstellten**.

In dem Papier wird insbesondere[52] Folgendes unterstrichen:

- *(Cloud-Anbieter) können keines der Prinzipien zum Schutz der Privatsphäre erfüllen, auf denen „Safe Harbour" gründet. Dieses Problem wurde von der Kommission vor dem überstürzten Abschluss des Abkommens trotz der Einwände europäischer DSB nicht zufriedenstellend gelöst. Infolgedessen bewerben viele US-Cloud-Anbieter ihre Safe-Harbour-Zertifizierung mit der unhaltbaren Behauptung, dass dadurch die Übermittlung von EU-Daten an US-Cloud-Anbieter legalisiert werde. Seit 2009 haben mehrere Anbieter ihre Anmeldung zur Selbst-Zertifizierung geändert und sich den widersinnigen Status eines Safe-Harbour-Anbieters verliehen, der als Datenverarbeiter agiert. In ihrem unlängst ergangenen Gutachten hat die Datenschutzgruppe nach Artikel 29 (WP29) klargestellt, dass dies unzureichend sei.*

- *Cloud-Anbieter sind transnationale Unternehmen und als solche internationalen Rechtskollisionen ausgesetzt. Nach welchem Recht sie sich richten, hängt von den im konkreten Fall anwendbaren Strafen und Erfordernissen und in der Praxis vom vorherrschenden Rechtsverständnis der Unternehmensleitung ab. Bislang galt das Interesse an solchen Konflikten beinahe ausschließlich dem US PATRIOT Act, doch wurden die Folgen des US-Gesetzes von 2008 zur Änderung des Gesetzes über die Überwachung der Auslandsgeheimdienste (FAA-Gesetz) quasi nicht angesprochen. Mit Paragraf 1881a des FAA-Gesetzes wurde erstmals eine Befugnis zur Massenüberwachung speziell von Daten von außerhalb der USA befindlichen Nicht-US-Personen geschaffen, die auch für Cloud Computing gilt. Obwohl alle Einzeldefinitionen aus früheren Gesetzen übernommen wurden, war die Kombination aller dieser Elemente neu .... die bedeutendste Änderung löste keine einzige Stellungnahme oder öffentliche Debatte aus. Der Überwachungsumfang wurde über das Abhören des Kommunikationsverkehrs hinaus auf alle Daten im öffentlichen Cloud Computing ausgeweitet. Diese Änderung ergab sich allein dadurch, dass „ausgelagerte Datendienste" in die Definition eines „Anbieters elektronischer Kommunikationsdienste" aufgenommen wurde.*

- *... weit reichende Folgen für die Datenhoheit der EU und den Schutz der Rechte ihrer Bürger. Die Folgen für die EU-Grundrechte leiten sich aus der Definition „ausländischer Geheimdienstinformationen" ab, zu denen Informationen über eine im Ausland ansässige politische Organisation oder ein ausländisches Hoheitsgebiet, die sich auf die Durchführung der Außenpolitik der Vereinigten Staaten beziehen, gehören. Anders ausgedrückt, in den USA kann rechtmäßig eine rein politische Überwachung der in US-Clouds zugänglichen Daten ausländischer Personen vorgenommen werden. Das Grundproblem besteht darin, dass Cloud Computing dem 40-jährigen Rechtsmodell für internationale Datenübermittlungen zuwiderläuft. Wünschenswert wäre primär ein umfassender internationaler Vertrag, der die volle Gegenseitigkeit der Rechte garantiert, doch könnten anderenfalls für besondere*

[51] Bigo Didier, Boulet Gertjan, Bowden Caspar, Carrera Sergio, Jeandesboz Julien, Scherrer Amandine (2012), Fighting cyber crime and protecting privacy in the cloud, Studie für das Europäische Parlaments, PE 462.509.

[52] Ähnlich starke Warnungen kamen von Hoboken, J.V.J., Arnbak, A.M., Van Eijk, N.A.N.M (2012)Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act, IVIR, Institute for Information Law, University of Amsterdam, November 2012 (englische Übersetzung). Siehe auch die Hinweise zur Unvereinbarkeit des FAA-Gesetzes mit der 2010 ergangenen Rechtsprechung des EGMR in: LoConte, Jessica (2010), FISA Amendments Act 2008: Protecting Americans by Monitoring International Communications--Is It Reasonable?, Pace International Law Review Online Companion 1-1-2010.

Umstände Ausnahmeregelungen unter der Voraussetzung getroffen werden, dass der konkreten Situation angemessene Schutzvorkehrungen bestehen. Cloud Computing verstößt gegen die Regel, dass Ausnahmen nicht zur Regel werden dürfen. Werden die Daten erst einmal an eine Cloud übermittelt, wird die Hoheit abgetreten. Zusammengefasst kann man sich nur schwer der Schlussfolgerung entziehen, dass die EU keine gebührenden Anstrengungen gegen einen unwiderruflichen Verlust von Datenhoheit unternimmt und zulässt, dass die bei den Verhandlungen zum Safe-Harbour-Abkommen von 2000 begangenen Fehler konsolidiert statt behoben werden.

- *Besondere Aufmerksamkeit sollte den US-Gesetzen zuteil werden, die die Überwachung von Cloud-Daten von nicht in den USA ansässigen Personen erlauben. Das EP sollte weitere Untersuchungen des US-amerikanischen Gesetzes zur Änderung des FISA-Gesetzes, des Status des 4. Zusatzartikels in Bezug auf Nicht-US-Personen und des USA PATRIOT Act (insbesondere Abschnitt 215) anfordern.*

- *Das EP sollte erwägen, die Datenschutzverordnung dahingehend zu ändern, dass vor dem Export von Cloud-Daten aus der EU in das Hoheitsgebiet der USA deutlich erkennbare Warnhinweise für betroffene Personen (die anfällig für eine politische Überwachung sind) vorgeschrieben werden. Die betroffenen Personen sollten nicht im Ungewissen gelassen werden, wenn sensible Daten zu ihrer Person gegenüber dem Überwachungsapparat eines Drittlandes offengelegt werden. Die bestehenden Ausnahmeregelungen müssen für Cloud-Dienste wegen des systemimmanenten Risikos des Verlusts der Datenhoheit außer Kraft gesetzt werden. Die EU sollten neue Verhandlungen mit den USA aufnehmen, damit diese das Menschenrecht auf Privatsphäre anerkennen, das Europäern gleichen Schutz vor US-Gerichten bietet.*

- *Die EU braucht eine Industriepolitik, die ihr Autonomie im Cloud Computing zugesteht. Die Mitteilung der GD INFSO vom Oktober 2012 wird in dieser Frage den hier analysierten Herausforderungen nicht gerecht. Eine Zielvorgabe könnte lauten, bis 2020 50 % der öffentlichen Dienste der EU auf der Basis einer Cloud-Infrastruktur zu betreiben, die einzig und allein der gerichtlichen Kontrolle der EU unterliegt.*

Ferner wurde in der Studie darauf hingewiesen, dass 2011 im Nachgang zur SWIFT-Affäre Gespräche zwischen einer „hochrangigen Kontaktgruppe“ der EU und den US-Behörden über ein Rahmenabkommen zur Regelung von Datenübermittlungen für Strafverfolgungszwecke stattfanden. Bislang beharren die USA darauf, dass dieses Abkommen sich nicht auf den Zugang von US-Behörden zu EU-Daten im Besitz nicht-öffentlicher US-Stellen erstrecken wird, was gerade den Fall des Cloud Computing ausschließen würde[53].

2.2.5. Nach FISA besteht für Nicht-US-Personen kein von den US-Behörden anerkanntes Recht auf Privatsphäre.

Der Erwerb *ausländischer Geheimdienstinformationen* im Rahmen des Programms PRISM setzt die Einhaltung der Verfahren zur „Minimierung“[54] und „Bestimmung von Zielpersonen“[55] voraus, die am 20. Juni (in unredigierter Form) vom *Guardian* enthüllt wurden. Gemeinsam betrachtet bieten diese Verfahren schlagkräftige Beweise dafür, dass es für Nicht-US-Personen nach PRISM und ähnlichen Programmen kein von den US-

[53] Datenschutzverhandlungen EU-USA:Non-Paper On Negotiations During 2011
[54] http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document
[55] http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document

Behörden anerkanntes Recht auf Privatsphäre gibt. Der Wortlaut dieser Dokumente ist von zahlreichen Wiederholungen geprägt und stark mit bürokratischem Jargon durchsetzt, doch auch bei eingehender Lektüre lässt sich keine Anerkennung der Rechte von Nichtamerikanern feststellen. Es ist daher zu vermuten, dass **für die Nutzung personenbezogener Daten einer Nicht-US-Person oder das Eindringen in ihre Privatsphäre in der operativen Praxis der USA keinerlei Einschränkung unterliegt, solange die allgemeine Definition *ausländischer Geheimdienstinformationen* zutrifft.**

Darüber hinaus stellt die Regierung in einem Schreiben vom Mai 2012 an die Kongressausschüssen zur Überprüfung der geheimdienstlichen Tätigkeit [56]

> *Da die NSA diesen Selektoren im Einklang mit ihren vom FISC genehmigten Verfahren für die Bestimmung von Zielpersonen bereits das Merkmal „ausländisch" zugewiesen hat, unterscheidet sich die diesbezügliche Rolle des FBI von der der NSA. Das FBI ist nicht gehalten, die Entscheidungen der NSA zur Bestimmung von Zielpersonen zu hinterfragen ...*

Die offengelegten Fassungen der Verfahren für die Bestimmung von Zielpersonen sind generisch formuliert, doch konnte die **American Civil Liberties Union** (**ACLU**)[57] (Amerikanische Bürgerrechtsunion) redigierte Exemplare von Powerpoint-Schulungsmaterial für FBI-Mitarbeiter erlangen, in denen für die Zwecke der Terrorismusbekämpfung konkret auf FISAAA Bezug genommen wurde. In dem Schreiben heißt es weiter:

> *Sobald alle Kommunikationsdaten erworben wurden, werden sie der NSA zugeleitet. Die NSA kann ferner festlegen, dass die im Rahmen von PRISM gesammelten Kommunikationsdaten für spezifische Selektoren auch an andere Bestandteile der Geheimdienstgemeinschaft abgezweigt werden.* (Hervorh. durch d. Verf.)

Das bedeutet, dass der CIA ebenso wie andere der 16 Agenturen der US-Geheimdienstgemeinschaft selbst Datenströme für die Speicherung und Analyse erhalten können, die bei der NSA einen Rohfilter nach einer Wahrscheinlichkeit eines „Auslandsmerkmals" in Höhe von 50 % durchlaufen haben. Diese „doppelte Abzweigung" oder der damit verfolgte Zweck wurden weder in den Berichten über Snowdens Dokumente noch in sonstigen Kommentaren erwähnt.

Gemäß den bekannt gewordenen „Verfahren zur Bestimmung von Zielpersonen" nach FAA (von 2009) wird auf eine NSA-Datenbank mit Telefonnummern und Internet-Identifkatoren[58] zurückgegriffen, um als Amerikaner bekannte Personen als ungewollte Zielpersonen nach Abschnitt 702 auszuschließen. Im nächsten Schritt dürfen Analysten nur dann nach Abschnitt 702 auf „Inhaltsdaten" zugreifen, wenn die Zielperson mit einer Wahrscheinlichkeit von mehr als 50 % Nichtamerikaner ist und sich außerhalb der USA befindet, da der 4. Zusatzartikel als nicht anwendbar angesehen wird. Andernfalls muss eine spezifische richterliche Anordnung gemäß einem anderen Abschnitt von FISA beantragt werden.

---

[56] https://www.aclu.org/files/assets/ltr_to_hpsci_chairman_rogers_and_ranking_member_ruppersberger_scan.pdf (am 21. August 2013 freigegeben)

[57] Antrag der ACLU auf Akteneinsicht nach dem Informationsfreiheitsgesetz (Freedom of Information Act, FOIA) (2010), Introduction to FISA Section 702, (2010),US-Justizministerium, Dezember 2010.

[58] Dabei handelt sich es anscheinend um eine andere Datenbank, ein Verzeichnis, nicht um die Metadaten, deren Erwerb nach Abschnitt 215 umstritten ist. Es ist nicht bekannt, wie (etwa durch Netzüberwachung) oder aufgrund welcher Befugnis die Datenbank zusammengestellt wird, doch stellt sie offensichtlich mehr als ein handelsübliches Telefonbuch dar.

Daran lässt sich erkennen, dass das Erfordernis eines „hinreichenden Verdachts“ als Nachweis für eine 50%ige Wahrscheinlichkeit *kriminellen Verhaltens* in eine 50%ige Wahrscheinlichkeit der *Nationalität*umgemünzt wurde. Diese Auslegung war zuerst aus einer 2008 ergangenen Entscheidung des FISA-Revisionsgerichts (FISCR) ersichtlich, die 2010 für kurze Zeit und in redigierter Form veröffentlicht und dann anscheinend von der offiziellen Website genommen wurde (eine Kopie[59] verblieb jedoch in den Händen einer im Bereich Transparenz tätigen NRO).

Das FISCR begründete den Entscheid so, dass**die von Auslandsgeheimdiensten betriebene Überwachung von Zielpersonen, bei denen ein hinreichender Grund zur Annahme besteht, dass sie sich außerhalb der USA befinden, für eine „bei besonderem Bedarf“ anzuwendende Ausnahme** [60] **vom Erfordernis einer richterlichen Anordnung nach dem 4. Zusatzartikel infrage kommen.** Die Verfassungsmäßigkeit dieses Urteils wird derzeit in mehreren von US-Bürgerrechtsorganisationen angestrengten Gerichtsverfahren angefochten, da dieses „umgekehrte“ Kriterium ein massives Abhören des Kommunikationsverkehrs von Amerikanern unter Verstoß gegen die Verfassung mit sich bringt.

2.3. Datenexport: falsche Lösungen und unzureichende Schutzvorkehrungen

Zum Abschluss dieses Kapitels möchte der Verfasser die Aufmerksamkeit des Parlaments auf bestimmte Schwierigkeiten im Zusammenhang mit derzeitigen Ausnahmeregelungen und/oder Schutzvorkehrungen lenken, die vorgeschlagen wurden, um Abhilfe in Bezug auf die oben unterstrichenen Folgen für EU-Bürger zu schaffen. In diesem Teilabschnitt sollen die Schlupflöcher und Lücken aufgezeigt werden, die bei mehreren für den Datenexport eingeführten Mechanismen bestehen. Nach Ansicht des Verfassers sollten diese Mechanismen nicht als Garant für den Schutz der Rechte von EU-Bürgern angesehen werden.

2.3.1 Safe-Harbour, Datenschutzregelungen für Datenverarbeiter und Cloud Computing

Mit dem im Jahr 2000 zwischen der EU und den USA geschlossenen Safe-Harbour-Abkommen wurde ein Prozess eingeführt, wonach US-Unternehmen der EU-Richtlinie 95/46/EG zum Schutz personenbezogener Daten nachkommen müssen. Wenn ein US-Unternehmen sich zur Einhaltung der **Grundsätze des Safe Harbour** verpflichtet, kann ein in der EU für die Datenverarbeitung Verantwortlicher Daten an dieses Unternehmen exportieren (auch wenn zusätzlich ein schriftlicher Vertrag vorgeschrieben ist).

Das bisweilen als „gleichzeitige einseitige Verpflichtungserklärung“ beschriebene Abkommen ließ offen, ob es auch für den Fall galt, dass die Datenverarbeitung auf Anweisung von für die Datenverarbeitung Verantwortlichen innerhalb der EU an Dienste innerhalb der USA ausgelagert wurde. Insbesondere im Fall des Cloud Computing waren diese Datenfernverarbeiter wohl kaum in der Lage, den Grundsätzen des Safe-Harbor-Abkommens Wirkung zu verleihen, das –so argumentierte die US-Seite – damit hinfällig wurde. Galt die Abmachung auch für den uneingeschränkten Export von EU-Daten für die Datenfernverarbeitung in einem Rahmen, der im Wesentlichen eine Selbstregulierung

[59] www.fas.org/irp/agency/doj/fisa/fiscr082208.pdfý

[60] Anzalda, Matthew A. and Gannon, Jonathan W. (2010), In re Directives...: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance (paywall), Texas Law Review, Vol 88:1599 2010.

vorgab? Im Jahr 2000 setzte sich die EU-Kommission über Einwände der Zivilgesellschaft und einiger DSB hinweg und schritt zum Abschluss des Abkommens.

Die Verhandlungsführer im US-Handelsministerium arbeiteten in enger Kooperation mit US-Handelslobbyisten an einer Reihe von „Häufig gestellten Fragen", um US-Unternehmen die Möglichkeit zur Auslegung des Abkommens unter marginaler Beachtung der EU-Rechte auf Privatsphäre zu bieten, indem sie Schlupflöcher in Fragen zu identifizierbaren Daten einbauten, Zugriffsrechte verweigerten und jegliche Verpflichtung auf Unanfechtbarkeit oder das Recht auf Löschung vermieden. Das Safe-Harbour-Abkommen erwies sich als so kompliziert, dass jahrelang kein EU-Bürger die bürokratischen Hürden für die Einreichung einer Beschwerde umschiffte.

In der 2004 im Auftrag der EU erstellten offiziellen Studie zur Überprüfung[61] von Safe Harbour wurde FISA nur kurz behandelt, die Bedeutung der oben erörterten *ausländischen Geheimdienstinformationen* für Nicht-US-Personen nicht untersucht und festgestellt, dass *„die umstrittenen Bestimmungen des USA PATRIOT Act im Wesentlichen irrelevant für den Datenverkehr im Rahmen von Safe Harbour"*seien.

Ein Großteil der rechtlichen Analyse, die die Hypothese von der Anwendbarkeit von Safe Harbour auf Cloud Computing stützt, lässt sich auf die Arbeit von Dr. Christopher Kuner[62]zurückführen, dem langjährigen Organisator einer Brüsseler Lobbygruppe, die sich aus Datenschutzbeauftragten von überwiegend multinationalen US-Konzernen zusammensetzt und bei der Kommission und den DSB an Einfluss gewonnen hat. Dr. Kuner vertrat außerdem die Internationale Handelskammer bei der Datenschutzdebatte in der EU und zählt als Berater große Internetunternehmen zu seinen Kunden. Kuners Lehrwerk zum europäischen Datenschutzrecht wurde in einer von Microsoft finanzierten Studie[63]mit dem Argument zitiert, dass Safe Harbour für die Datenverarbeitung in der Cloud ausreichend sei. Diese Auffassung wurde unlängst von den USA ausdrücklich bekräftigt[64].

Vor diesem Hintergrund nahm eine DSB-Arbeitsgruppe um 2009 Gespräche mit großen Internetkonzernen über eine neue geplante Ausnahmeregelung auf, die sich auch auf Cloud Computing erstrecken könnte und als v*erbindliche unternehmensinterne Vorschriften für Datenverarbeiter* bekannt wurde.

Dahinter stand der Gedanke, dass ein in den USA (oder einem Drittland) ansässiger Cloud-Diensteanbieter eine Sicherheitsbescheinigung für eine gesamte Software-Plattform bei einem anerkannten Prüfer einholen und ein für die Verarbeitung Verantwortlicher in der EU unter Verwendung einer von WP29 erarbeiteten „Checkliste" organisationsinterner Verfahren[65] anschließend rechtmäßig personenbezogene Daten aus der EU heraus in die unter ausländischer Kontrolle stehende Cloud exportieren könnte. Die in der Checkliste

[61] Dhont J., Asinari M.V.P., Poullet Y., Reidenberg J., Bygrave L. (2004), Safe Harbour Decision Implementation Study, Europäische Kommission, Auftrag der GD Binnenmarkt PRS/2003/A0-7002/E/27.

[62] Kuner, Christopher (2008), Membership of the US Safe Harbor Program by Data Processors, The Center For Information Policy Leadership, Hunton & Williams LLP.

[63] Hon, W. Kuan and Millard, Christopher (2012), Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4, QMUL Cloud Legal Project: „Es besteht eine gewisse Unsicherheit darüber, ob der Safe-Harbor-Rahmen auf Datenübermittlungen an einen US-Datenverarbeiter (im Gegensatz zu einem für die Datenverarbeitung Verantwortlichen), etwa einen Cloud-Diensteanbieter, anwendbar ist. Es spricht mehr dafür, dass dem so ist..." Siehe auch Walden, Ian (2011), Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, QMUL Cloud Legal Project, Research Paper No. 74/2011, Fußnote 119.

[64] US-Handelsministerium, Behörde für Internationalen Handel (2013), Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing.

[65] ART29WP – Artikel-29-Datenschutzgruppe (2012), Arbeitsdokument 02/2012 mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter, WP 195, angenommen am 6. Juni 2012.

erteilten Auflagen und enthaltenen Formulierungen ähnelten denen, die von der Kommission bereits für Standardvertragsklauseln (siehe unten) erarbeitet worden waren (und stärkten sie in begrenztem Umfang).

Möglicherweise in Reaktion auf warnende Hinweise zu FISA veröffentlichte WP29 zwei Monate vor der Snowden-Affäre eine scheinbar unwesentliche „Klarstellung" mit der ergänzenden Bemerkung,[66] dass die Checkliste

> *"**lediglich** ein Informationsverfahren vorsehen, das die Weitergabe nicht per se legitimiert. Bei Rechtskollisionen **ist** ist auf die für diesen Bereich geltenden internationalen Verträge und Vereinbarungen **zu verweisen**."* [Hervorh. d. Verf.].

Es erscheint nicht sehr klug, die Bürde der Verantwortung für eine derart wichtige Bewertung[67]internationaler Rechtskollisionen auf ein ausländisches Unternehmen mit starkem Eigeninteresse abzuwälzen, das befürchten muss, aufgrund der Einhaltung des EU-Rechts wegen Spionage angeklagt zu werden.

Verbindliche unternehmensinterne Datenschutzregelungen (Binding Corporate Rules, BCR) für Datenverarbeiter hören sich vielleicht an wie eine Variante der bestehenden BCR (für die für Datenverarbeitung Verantwortlichen), bergen jedoch tatsächlich ein weitaus größeres Risiko für die Privatsphäre von Europäern. **Das strategische Risiko für die Datenhoheit der EU, das unmittelbar aus dem Konzept der „BCR für Datenverarbeiter" erwächst, besteht darin, dass die globale Cloud-Industrie von Software-„Plattformen" Microsofts, Googles, Amazons und einiger weniger anderer Konzerne beherrscht wird.** Microsoft stellte 2010 für sein Vertriebsteam für den öffentlichen Sektor das Ziel auf, sich um jeden von Regierungen ausgeschriebenen Verarbeitungsauftrag zu bewerben[68]. **Die Cloud-Verarbeitung ermöglicht massive Kosteneinsparungen (den Werbebehauptungen der Branche zufolge mitunter ein Zehntel der Kosten der „internen" Verarbeitung durch den für die Verarbeitung Verantwortlichen). Diese Einsparungen entstehen bei der Ausrüstung, der Verwaltung und dem Betriebspersonal (die Kosten führender Experten im Bereich Computersicherheit steigen immer mehr). Zudem können große Cloud-Anbieter von Größenvorteilen und einer höheren durchschnittlichen Auslastung durch die globale Verteilung der Verarbeitungslasten auf mehrere Zeitzonen profitieren. Daher gebietet es der Wettbewerb bereits jetzt und auch künftig, europäische Daten aus der „internen" Verarbeitung in die Cloud-Verarbeitung zu migrieren, doch verfügt die EU bislang über so gut wie keinen eigene nennenswerten Software-Plattformen, die sich (in Bezug auf Kosten, Merkmale oder Zuverlässigkeit) mit denen der führenden US-Anbieter messen können. Eine Ausnahme von diesem düsteren Bild bildet freie und quelloffene Software, die leistungsstarke, mit proprietärer Software und Diensten konkurrenzfähige „Cloud Stacks" hervorgebracht hat.**

In diesem Licht können BCR für Datenverarbeiter als eine zweckdienliche Strategie sowohl für die Kommission als auch für die Datenschutzbehörden (DSB), die den Anschein einer legalen Kontrolle über EU-Daten aufrechterhalten möchten, und für die Cloud-Anbieter angesehen werden, die die bestehenden EU-Datenschutzregelungen allgemein als

[66] ART29WP – Artikel-29-Datenschutzgruppe (2013), Erläuterndes Dokument zu verbindlichen unternehmensinternen Datenschutzregelungen für Auftragsverarbeiter, WP 204, angenommen am 19. April 2013.

[67] Eine einschlägige Erörterung solcher Rechtskollisionen findet sich bei: Radsan, John A. (2007), The Unresolved Equation of Espionage and International Law, Michigan Journal of International Law, Vol 28:595 2007.

[68] Der Verfasser war bis 2011 leitender Datenschutzberater für die 40 nationalen (für die Verbindung zur Regierung zuständigen) Technologiereferenten von Microsoft und erhielt eine spezielle Vertriebsschulung mit Schwerpunkt auf dem für Cloud-Dienste gestellten Ziel, sich um alle Regierungsaufträge ungeachtet der Sensibilität der Daten zu bewerben. Auf die Anfrage, ob dies ein Fehler sei, wurde das Ziel bekräftigt.

hinderlich empfinden, insbesondere für steuerliche Zwecke[69]. Die Kommission hob den rechtlichen Status der BCR für Datenverarbeiter im Wortlaut des neuen Verordnungsentwurfs an[70]. Demzufolge bliebe den nationalen DSB nichts anderes übrig, als ihre Gültigkeit nach ihrem Erlass zu akzeptieren. Bislang wurden nur einige Dutzend der vorhandenen BCR für die für die Verarbeitung Verantwortlichen gebilligt[71], doch schon jetzt ist der Stand der Einhaltung beunruhigend[72].

2.3.2. Standardverträge

Seit 2001 erarbeitet die EU-Kommission gebilligte „Standardklauseln", die zur Aufnahme in Verträge sowohl für die für Datenverarbeitung Verantwortlichen als auch für Datenverarbeiter außerhalb der EU bestimmt sind und für den Einzelnen ähnliche Persönlichkeitsrechte wie bei einem Verbleib der Daten in der EU gewährleisten sollen.

Der konzeptionelle Mangel dieses allgemeinen Ansatzes besteht in der Annahme, dass Computersysteme auf die Gewährleistung der drei wesentlichen Erfordernisse der Informationssicherheit „geprüft" werden können: Vertraulichkeit, Integrität und Verfügbarkeit. Während Integrität[73] und Verfügbarkeit von Daten technisch und logisch überprüfbare Merkmale darstellen, lässt sich das von Vertraulichkeit nicht sagen. Es ist unmöglich, mit Gewissheit zu bestimmen, ob entweder ein „Insider" oder ein unbefugter Externer Daten eingesehen oder kopiert hat. Selbst wenn die Daten mit einer mathematisch starken Chiffrierung verschlüsselt sind, kann es vorkommen, dass die Algorithmenentwicklung mit Softwarefehlern behaftet ist oder der Schlüssel heimlich weitergegeben oder gestohlen wird.

Die Enthüllungen über PRISM führen eindrucksvoll vor Augen, wie unsinnig dieser juristische Schachzug ist. Keine Rechtskraft, auf die sich nichtöffentliche Stellen in zivilrechtlichen Fällen berufen, kann angesichts eines Gegners wie der NSA Persönlichkeitsrechte gewährleisten, wenn dieser versucht, dagegen zu verstoßen, und dabei von der Rechtmäßigkeit seines Handelns ausgeht.

Klausel 5 Buchstabe d Ziffer i[74] sah vor, dass der Datenverarbeiter den EU-Exporteur unverzüglich über „alle rechtlich bindenden Aufforderungen" zur Weitergabe von Daten informiert, **es sei denn**, dies wäre anderweitig untersagt, **wie zum Beispiel** ein strafrechtliches Verbot, um die Vertraulichkeit einer Untersuchung bei strafrechtlichen Ermittlungen zu gewährleisten. Die Formulierung „wie zum Beispiel" lädt zu der

[69] Große US-amerikanische Internetkonzerne neigen zur Praxis des „Forum-Shopping" bei Mitgliedstaaten, um sich Vorteile durch niedrige Steuern und schwache Datenschutzregelungen zu verschaffen. Wenn diese nicht übereinstimmen, muss der Unternehmensanwalt überaus komplexe Verträge ausarbeiten, um sie mit den technischen Details von „Standardverträgen" in Einklang zu bringen.

[70] BCR (Art. 43) werden nicht länger als „Ausnahme" (Art. 44) eingestuft; siehe: Europäische Kommission (2012), Vorschlag für eine Datenschutz-Grundverordnung, 25.1.2012, COM(2012) 11 final 2012/0011.

[71] Eine kurze Stichprobe bei einem Dutzend dieser Unternehmen ergab, dass die meisten nicht – wie vorgeschrieben – die tatsächlichen BCR-Konditionen online verfügbar machen.

[72] Der Verfasser reichte bei der DBS Luxemburgs Beschwerde darüber ein, dass das für Datenschutz zuständige Personal von PayPal keine Kenntnis von BCR besaß (PayPal kann die BCR-Konditionen nicht einhalten, wenn seine Mitarbeiter nicht einmal wissen, dass es sie gibt und welche Verpflichtungen sie umfassen). Trotz mehrerer Mahnungen ist ein Jahr später noch immer nichts über das Ergebnis der Untersuchung bekannt.

[73] Zur Integritätsprüfung wird für die Daten eine „Hashfunktion" erzeugt, die als überprüfbarer „Fingerabdruck" fungiert.

[74] Entscheidung der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (2002/16/EG).

Interpretation ein, dass nationale Sicherheitsgesetze*folglich* jeglichen vertraglichen Pflichten übergeordnet seien. Obwohl die EU das Recht des Datenexporteurs auf Rücktritt vom Übermittlungsvertrag beibehielt, ist für einen solchen Rücktritt eine Beweisgrundlage erforderlich, und somit wurde die Versuchung, darüber hinwegzusehen, strukturell eingebaut.

Jeder Organisationsakteur hat nach diesen Regelungen einen Anreiz, die Augen zu verschließen. Die Kommission, damit sie die Einhaltung „hoher Auflagen" für den Datenschutz behaupten kann; die DBS, damit ihre technischen Grenzen nicht bekannt und ihre begrenzten Mittel nicht in kostspieligen Gerichtsverfahren erschöpft werden; die Mitgliedstaaten, deren Sicherheitshierarchien vom Zugriff auf die US-Informationen zur Terrorismusbekämpfung profitieren; und die Unternehmen in der EU und den USA, die einfach nur Geschäfte führen wollen, ohne dass immer wieder unangenehme Fragen zur staatlichen Massenüberwachung auftreten. Selbst die Zivilgesellschaft der EU[75] blieb in Anbetracht von ECHELON untätig und widmete sich vor allem den Verbraucherrechten[76], statt die Folgen für die Grundrechte und die Hoheit im kommerziellen Datenverkehr in die USA sinnvoll zu hinterfragen.

Als Rechtsmechanismus zur Gewährleistung von Rechten und zur Erlangung von Schadenersatz bei mangelhaften Sicherheits- oder Datenschutzpraktiken haben sich derartige Verträge (und ihre „Standardklauseln") insofern als nutzlos erwiesen, als sie nicht zu Rechtsstreitigkeiten geführt haben. In den meisten Fällen, in denen ein für die Datenverarbeitung Verantwortlicher in der EU möglicherweise die Zahlung von Schadensersatz durch einen Datenverarbeiter oder einen für die Verarbeitung Verantwortlichen eines Drittlandes anstrebt, ließe sich sein Ansehensverlust am Markt (z. B. durch das Bekanntwerden einer Verletzung der Datensicherheit) wohl kaum wiedergutmachen. Theoretisch würde sich diese abschreckende Wirkung mit dem im Entwurf der neuen Regelungen vorgesehenen Erfordernis[77], Sicherheitsverletzungen an die DSB zu melden, nicht länger entfalten, doch haben die DSB ihre Absicht kundgetan, nicht unbedingt zu verlangen, dass die Betroffenen informiert werden (und somit der Vorfall öffentlich bekannt wird), teilweise um die für die Verarbeitung Verantwortlichen vor einem unverhältnismäßigen Imageschaden zu bewahren. Eine außergerichtliche und nicht öffentlichkeitswirksame Regelung vertraglicher Rechtsstreitigkeiten unterhöhlt die Funktion, die diesen Streitigkeiten zukäme, nämlich die für die Verarbeitung Verantwortlichen über die Zuverlässigkeit derjenigen zu informieren, an die sie möglicherweise Daten exportieren. Falls es zu einer Beeinträchtigung der Rechte der Betroffenen nach diesem Ansatz gekommen sein sollte, erfahren die Betroffenen natürlich nichts davon.

[75] Eine nennenswerte Ausnahme bildet der Chaos Computer Club in Deutschland.

[76] Wobei es optimistisch stimmende Ausnahmen wie die kurzlebige „International Campaign Against Mass Surveillance" von 2005 gibt (die Website ist nicht mehr aktiv, eine Kopie ist jedoch hiergespeichert) und in der Zivilgesellschaft Deutschlands allgemein ein hohes Maß an Wachsamkeit herrscht, das im Sinne der Vermeidung von Wiederholungen als selbstverständlich anzusehen ist.

[77] .Das derzeitige Erfordernis zur Meldung von Sicherheitsverletzungen nach der überarbeiteten Datenschutzrichtlinie gilt nur für Telekommunikationsunternehmen und Anbieter von Internetdiensten, nicht jedoch für Dienste der Informationsgesellschaft, die über Websites wie soziale Netze und Suchmaschinen und allgemein für die Datenverarbeitung Verantwortliche bereitgestellt werden.

3. STRATEGISCHE OPTIONEN UND EMPFEHLUNGEN FÜR DAS EUROPÄISCHE PARLAMENT

3.1. Verringerung der Angreifbarkeit und Aufbau einer europäischen Cloud

Wie bereits zuvor erläutert, ist der Mechanismus der BCR für Datenverarbeiter scheinbar maßgeschneidert für die Erleichterung des Datenverkehrs von der EU in das Cloud Computing eines Drittlandes, schützt aber die Rechte nicht in ausreichendem Maße. Er enthält ein Schlupfloch, das eine unrechtmäßige Überwachung zulässt. Es ist daher recht überraschend, dass das Konzept in mehreren Phasen seiner Entwicklung die Billigung der Artikel-29-Datenschutzgruppe[78] (WP29), des Europäischen Datenschutzbeauftragten[79] (EDSB) und der französischen *Commission Nationale de l'Informatique et des Libertés* (CNIL) fand, die seine Ausgestaltung anleiteten. Es gibt keine Belege dafür, dass diese DSB die strukturelle Verlagerung der Datenhoheit[80], die das Cloud Computing mit sich bringt, erkannt haben. Vielmehr hat eine unrealistische und legalistische Perspektive eine Vernachlässigung des Schutzes der EU-Bürger ermöglicht.

Empfehlungen:

- Jede US-Website, die Dienste in der EU anbietet, sollte deutlich sichtbare Hinweise darauf enthalten, dass EU-Bürger nach erfolgter Aufklärung in die Sammlung ihrer Daten einwilligen können. Die Nutzer sollten darauf aufmerksam gemacht werden, dass die Daten von der US-Regierung (nach FISA-Abschnitt 702) zu jedem ihrer Außenpolitik förderlichen Zweck überwacht werden können. Mit einem Einwilligungserfordernis wird der EU-Bürger stärker sensibilisiert und das Wachstum von Diensten unter der ausschließlichen Rechtshoheit der EU begünstigt. Dies wiederum wird wirtschaftliche Auswirkungen auf die US-Unternehmen haben und die US-Regierung stärker unter Druck setzen, eine Einigung herbeizuführen.

- Da die anderen Hauptmechanismen für den Datenexport (Standardverträge, Safe Harbour) keinen Schutz vor FISA oder PATRIOT bieten, sollten sie aufgehoben und neu verhandelt werden. Auf jeden Fall sollte das genannte Erfordernis der Einwilligung nach erfolgter Aufklärung durch einen deutlich sichtbaren Warnhinweis für alle Daten gelten, die von für die Datenverarbeitung Verantwortlichen des öffentlichen oder privaten Sektors der EU in der Vergangenheit gesammelt wurden oder künftig gesammelt werden, bevor sie zur Cloud-Verarbeitung in die USA exportiert werden können.

- Es sollte ein umfassendes branchenspezifisches Politikkonzept für die Entwicklung einer eigenständigen europäischen Kapazität für Cloud Computing auf der Grundlage freier/quelloffener Software unterstützt werden. Ein solches Politikkonzept würde die Kontrolle der USA über die oberen Segmente der Wertschöpfungskette im cloudbasierten elektronischen Geschäftsverkehr und der Online-Werbemärkte der EU verringern. Derzeit unterliegen europäische Daten der gewerblichen Manipulation,

[78] ART29WP – Artikel-29-Datenschutzgruppe (2012), Stellungnahme zum Cloud Computing, WP 196, angenommen am 1. Juli 2012.
[79] Europäischer Datenschutzbeauftragter – Hustinx, Peter (2010), Datenschutz und Cloud Computing nach dem EU-Recht, Rede auf dem Dritten Europäischen Tag zur Sensibilisierung für Fragen der Netzsicherheit, BSA, Europäisches Parlament, 13. April 2010, Panel IV: Privatsphäre und Cloud Computing.
[80] De Filippi, Primavera, and McCarthy, Smari (2012), Cloud Computing: Centralization and Data Sovereignty, European Journal of Law and Technology 3, 2.

der Überwachung durch Auslandsnachrichtendienste und der Industriespionage. Investitionen in eine europäische Cloud werden wirtschaftliche Vorteile bringen und die Grundlage für eine dauerhafte Datenhoheit bilden.

3.2. Wiederaufnahme von „Artikel 42“

In der veröffentlichten[81] neuen Verordnung entfiel „Artikel 42“ (nach der Zählung in einem Entwurf[82], der zwei Monate vor Erscheinen der endgültigen Fassung an die Öffentlichkeit gelangte), angeblich nach höchst intensiver Lobbyarbeit US-amerikanischer Interessenträger[83]. Artikel 42 verbietet Drittländern (wie den USA und anderen Nicht-EU-Mitgliedern) den Zugriff auf personenbezogene EU-Daten, die von einem Gericht oder einer Verwaltungsbehörde außerhalb der EU angefordert werden, es sei denn, eine EU-Datenschutzbehörde hat zuvor ihre Genehmigung erteilt. Dieser Artikel wurde als „Anti-FISA-Klausel“ beschrieben.

Empfehlungen: Vor seiner Wiederaufnahme sollte „Artikel 42“ auf seine abschreckende Wirkung untersucht werden. Dabei sollten insbesondere folgende Punkte angesprochen werden:

- Zwar werden die kontroversen Aspekte von FISA durch Artikel 42 im Prinzip gemildert, doch sind Zweifel an der Wirksamkeit dieser Maßnahme angebracht, da die Leitung von US-Unternehmen bei einer Einhaltung der Bestimmungen Anschuldigungen wegen Spionage befürchten müsste. Die Geschäftsführerin von Yahoo erklärte unlängst: „*Uns würde eine Gefängnisstrafe drohen, wenn wir die Überwachungsgeheimnisse der NSA offenbarten.*“[84]

- Die Effizienz von Sanktionen als Mechanismus zur Durchsetzung der Einhaltung sollte auch unter dem Blickwinkel des wirtschaftlichen Nettogewinns und -verlusts bewertet werden. Um ein Beispiel zu nennen: Die EU-Wettbewerbsbehörde verfolgte Microsoft in einem langwierigen Fall wegen seines Monopols bei lokalen Netzwerken und verhängte ein Bußgeld in Höhe von 1 Mrd. USD (die höchste je von der EU geforderte Strafzahlung). Der für diese Strategie zuständige Unternehmensanwalt wurde nicht wegen Inkompetenz entlassen, sondern zum stellvertretenden Chefjustiziar befördert. Grund dafür ist, dass Microsofts Gewinne aus dieser Monopolstellung im letzten Jahrzehnt nach vorsichtigen Schätzungen das 20-fache der riesigen Geldstrafe betrugen, was die Rechtsstrategien des Konzerns vorausgesehen hatten.

- Sollte ein großer Cloud-Anbieter dem Artikel 42 nicht nachkommen, könnte das zu einer unumkehrbaren, aber geheimen Verletzung der Grundrechte von Millionen von Bürgern führen, und die Verordnung sollte dies als gravierenden Straftatbestand deklarieren. Derzeit werden Verstöße gegen Datenschutzauflagen in den meisten Rechtsvorschriften der Mitgliedstaaten zur Umsetzung der EU-Richtlinie 95/46/EG als geringfügig bewertet. Einige Mitgliedstaaten wenden überhaupt keine strafrechtlichen Sanktionen an. Dies wirkt nicht abschreckend auf eine kalkulierte, gegen die nach US-Recht anwendbaren Strafen abgewogene Strategie zur Missachtung des EU-Rechts.

---

[81] Europäische Kommission (2012), Vorschlag für eine Datenschutz-Grundverordnung, 25.1.2012, COM(2012) 11 final 2012/0011.
[82] Europäische Kommission (2011), [Draft] Proposal for a General Data Protection Regulation
[83] Washington pushed EU to dilute data protection, *Financial Times*, 12. Juni 2013.
[84] The Guardian, 12. September 2013, http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance?CMP=twt_gu

- Allgemein und über den konkreten Geltungsbereich von Artikel 42 hinaus ist auch eine deutliche Erhöhung der Geldbußen für Verstöße gegen die neue Datenschutzverordnung erforderlich, die gegenüber höheren Beträgen in durchgesickerten Entwürfen auf eine Strafe in Höhe von 2 % des Umsatzes des Unternehmens gesenkt wurden. Wie das oben angeführte Beispiel der Wettbewerbsklage gegen Microsoft deutlich macht, verfügen einige Unternehmen über riesige Ressourcen und durchdachte Strategien, dank deren sie selbst Bußgelder in Milliardenhöhe voraussehen und bei ihrer Geschäftsplanung berücksichtigen. Möglicherweise bedarf es eines Bußgelds in Höhe von 20 % des globalen Umsatzes, um diese Unternehmen davon zu überzeugen, die Einhaltung von Artikel 42 ernst zu nehmen.

- Selbst nach BULLRUN ist die Kryptografie theoretisch wahrscheinlich intakt[85], doch ist nicht bekannt, welche Verschlüsselungsanwendungen und -produkte ausgehebelt wurden. **Daher sollte in Erwägung gezogen werden, den Geltungsbereich von „Artikel 42" (über die für die Verarbeitung Verantwortlichen/Verarbeiter hinaus) auf die Anbieter von Systemen/Produkten auf EU-Märkten auszuweiten.** Vorhandene Sicherheitsbescheinigungen für Verschlüsselungsprodukte, insbesondere wenn sie dem Einfluss der NSA oder des GCHQ unterlagen, müssen als verdächtig angesehen werden.

3.3. Schutz von Hinweisgebern und entsprechende Anreize

Empfehlung: In die neue Verordnung sollten Regelungen für den systematischen Schutz von Hinweisgebern („Whistleblowern") und entsprechende Anreize Eingang finden. Den Hinweisgebern sollten Immunität und Asyl fest zugesagt und 25 % einer in der Folge verhängten Geldstrafe zugesprochen werden[86]. Hinweisgeber müssen möglicherweise lebenslange Vergeltung in ihrem Land befürchten und Vorkehrungen treffen, um einer „außerordentlichen Überstellung" (Entführung) zu entgehen. Ironischerweise sieht das US-Recht bereits Belohnungen in Höhe von 100 Mio. USD für Hinweisgeber vor, die Korruption (im Bereich öffentliche Beschaffung und Preisfestsetzung) aufdecken[87].

3.4. Institutionelle Reform

In einer sehr frühen Phase der Konsultationen verwarf die EU-Kommission die Option, eine neue zentrale Datenschutzbehörde für ganz Europa einzusetzen, da dies im Hinblick auf die Subsidiarität der Mitgliedstaaten unverhältnismäßig erschien. Man entschied sich für die Weiterentwicklung der WP29 zum neuen Datenschutzausschuss. Es wäre allerdings möglich gewesen, eine Zwischenlösung in Erwägung zu ziehen: die Schaffung einer neuen zentralen Behörde für Fälle umfangreichen Datenverkehrs mit Drittländern.

Empfehlung: Es sollte ein zentraler Ermittlungsdienst für Fälle umfangreichen Datenverkehrs mit Drittländern geschaffen werden. Dieser Dienst sollte die Befugnis und die Mittel erhalten, komplexe Ermittlungen gegen transnationale Unternehmen einzuleiten, die häufig zahlreiche Rechtsberater einstellen, um Entscheidungen jahrelang

[85] Anderenfalls würde die NSA nicht so viele Ressourcen für ihre Umgehung auf indirektem Weg aufwenden (sofern es sich dabei nicht um Täuschungsmanöver von enormem Ausmaß handelt).
[86] Dieses Verfahren ist im Recht seit Langem unter der Bezeichnung Qui Tam bekannt.
[87] http://www.theguardian.com/business/2010/oct/27/glaxosmithkline-whistleblower-wins-61m

hinauszuzögern und anzufechten. Die DSB würden die Rechtshoheit über rein nationale Angelegenheiten behalten und könnten nach dem Subsidiaritätsprinzip selbst nationale Ermittlungen aufnehmen oder einen Fall an den zentralen Dienst verweisen.

3.5. Datenschutzbehörden und -kontrolle

Der PRISM-Skandal und die Enthüllungen Snowdens waren nicht die ersten Warnsignale für die EU-Organe, was die Rechte von EU-Bürgern anbelangt. So haben Datenschützer die Kommission im Jahr 2000 auf die gefährlichen Schlupflöcher im Safe-Harbour-Abkommen hingewiesen[88]. Vor noch kürzerer Zeit wurde im oben genannten Papier zum Cloud Computing, das für den LIBE-Ausschuss des Europäischen Parlaments erstellt worden war, klar auf die Schlupflöcher von FISA und ihre Folgen für die Rechte und den Schutz von EU-Bürgern aufmerksam gemacht[89].

Der Ausschuss hielt nach einer Sitzung über die Cybersicherheitsstrategie der EU am 20. Februar 2013 sogar eine Anhörung[90] zur Vorstellung des Papiers ab. Anschließend baten Mitglieder des Europäischen Parlaments um unverzügliche Vorschläge zur Einhaltung der Frist für vom LIBE-Ausschuss einzubringenden Anträge zur Änderung[91] der Datenschutzverordnung. Ab März ließ das Interesse an dem Papier allerdings nach, und die Möglichkeit, dass das Parlament grundlegende Überarbeitungen der Datenschutzverordnung unterstützen würde, rückte in weite Ferne. Es ist dem PRISM-Skandal und den Enthüllungen von Snowden zu verdanken, dass diese Warnungen und damit zusammenhängenden Besorgnisse erneut ernst genommen werden. Es bleibt die Frage, warum die DSB nicht reagiert haben.

Nur in einer der 150 Stellungnahmen, die WP29 seit dem 11. September 2001 herausgegeben hat, wird der PATRIOT Act (in einer Fußnote) erwähnt, FISA oder auch nur der Begriff „ausländische Geheimdienstinformationen“ dagegen in keiner. Den nationalen DSB[92], dem EDSB[93] und anderen Institutionen[94] war offenbar nicht bekannt, dass solche US-Rechtsvorschriften existierten oder dass PRISM rechtlich möglich war. Sie versäumten es, die Alarmglocken für die EU-Bürger zu läuten, obwohl es bereits vor 2008 warnende Hinweise[95] und natürlich zahlreiche Meldungen zum US-Skandal gegeben hatte. Das mag daran gelegen haben, dass die DSB, die ENISA[96] und das Referat „Vertrauen und Sicherheit“ der GD CONNECT[97] unschlüssig

[88] Der Verfasser (damals Direktor von FIPR) und andere richteten an Amtsträger die Frage, ob Safe Harbour eine Massenüberwachung nach der Art von „ECHELON“ gestatte, erhielten jedoch keine Antwort.

[89] Bigo Didier, Boulet Gertjan, Bowden Caspar, Carrera Sergio, Jeandesboz Julien, Scherrer Amandine (2012), Fighting cyber crime and protecting privacy in the cloud, Studie für das Europäische Parlament, PE 462.509.

[90] Anhörung des LIBE-Ausschusses des Europäischen Parlaments vom 20. Februar 2013 zur Computerkriminalität/Cloud-Bericht (Video ab 17:08:18).

[91] Die vom LIBE-Ausschuss eingebrachten Anträge 806/2531/2748/2950 zur Änderung der neuen Verordnung gehen auf diese Vorschläge zurück.

[92] Mit Ausnahme der deutschen DSB, die wachsam waren. Siehe Weichert, Thilo (2011), Cloud Computing and Data Privacy, The Sedona Group Conference Working Group Series, Februar 2011. Siehe auch: International Working Group on Data Protection in Telecommunications (2012), Arbeitspapier Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes – „Sopot Memorandum“ , 51. Sitzung, 23.-24. April 2012.

[93] Bowden, Caspar (2012), Is EU data safe in US Clouds? (Powerpoint-Präsentation), Europäische Rechtsakademie Trier, September 2012. Sowohl der EDSB als auch sein Stellvertreter sowie leitende Beamte des Rates, der Kommission und anderer DSB waren anwesend und erhielten anschließend eine Kopie per E-Mail.

[94] Siehe 28.6.12 - Anhörung der Europäischen Grünen Partei zum Datenschutz (Powerpoint-Präsentation) (t=2h43m); siehe auch: 10.10.12 Interparlamentarisches Forum des LIBE-Ausschusses.

[95] Bowden, Caspar (2011), Government Databases and Cloud Computing (Powerpoint-Präsentation), The Public Voice, Mexiko, Oktober 2011.

[96] Am 14.6.2013 beantwortete die ENISA-Pressestelle eine Frage des Verfassers an den Direktor dahingehend, dass eine Verteidigung gegen die NSA außerhalb ihres Mandats liege, gab jedoch – wohl in der Einsicht der

waren, ob die Ausnahme von der EU-Zuständigkeit aus Gründen der „nationalen Sicherheit“ bedeutet, dass sie die Privatsphäre ihrer Bürger gegen Geheimdienste von Drittländern verteidigen sollen oder nicht verteidigen müssen.

In der letzten Stellungnahme zum aktuellen Stand, die der EDSB vor der Snowden-Affäre abgab, nahm er Kenntnis vom oben genannten Antrag des LIBE-Ausschusses, den Entwurf im Hinblick auf eine drastische Warnung der Betroffenen vor ihrer Einwilligung in Cloud-Datenübermittlungen abzuändern, wies ihn jedoch mit der Begründung zurück[98], er sei nicht „technologieneutral“.

Bei den DBS-Institutionen der EU bestehen offensichtlich strukturbedingte Schwierigkeiten, die es anzugehen gilt. Insbesondere fehlt es ihnen eindeutig an Kapazitäten für den technischen Sachverstand. Nur einige Dutzend DSB-Mitarbeiter (von etwa 2000 in ganz Europa) verfügen über solide Informatikkenntnisse geschweige denn über einen informations- oder ingenieurwissenschaftlichen Postgraduiertenabschluss im Bereich Datenschutz. Es hat sich die Ansicht durchgesetzt, dass Regulierungsbehörden aufgrund einer allgemeinen Präferenz für die Abfassung von Gesetzen auf technologieneutrale[99] Weise vom Verständnis technischer Fragen freigestellt seien. So hat WP29 bislang keine Umfrage zu fortschrittlichen datenschutzfreundlichen Technologien durchgeführt oder in einer Stellungnahme ein Mandat für ihren Einsatz erteilt, nicht einmal angesichts anhaltender Beweise dafür, dass der Markt in Bezug auf ihre freiwillige Annahme versagt hat.

Empfehlungen: Das Stellenbesetzungssystem der EU-Datenschutzbehörden sollte reformiert werden. Die neue Verordnung geht auf diesen Aspekt nicht ein. Dies ist eine entscheidende Voraussetzung für die Vermeidung von Trägheit und Stillstand in Bezug auf technologiespezifische Fragen. Einige Optionen zur Verbesserung der Datenschutzkontrolle und -kapazitäten in der EU könnten wie folgt lauten:

- Aufnahme mindestens eines Sonderbeauftragten in den Datenschutzausschuss mit dem Mandat, die Verteidigung der Rechte der Bürger zur Priorität zu erheben, und mit einem kleinen und unabhängigen Mitarbeiterkreis, möglicherweise in direkter Wahl durch mehrheitliches (jedoch apolitisches) Votum zum Zeitpunkt der Europawahlen oder durch das Parlament;

- Aufnahme eines technischen Sonderbeauftragten, der aus dem Kreis akademischer Informatiker mit Spezialisierung in Datenschutz benannt wird, und potenziell eines weiteren Beauftragten aus dem Bereich Überwachungsstudien, ebenfalls mit einem kleinen und unabhängigen Team von Mitarbeitern;

- die Festlegung, Datenschutzbeauftragte von nationalen Parlamenten, nicht von der Exekutive ernennen zu lassen;

Unhaltbarkeit dieser Position – am 6.9.2013 eine präzisierende Erklärung ab, in der (in Fußnote 21) unrichtigerweise impliziert wurde, die ENISA habe 2009 vor FISA-ähnlichen Risiken gewarnt.

[97] Erklärung eines zuständigen Beamten der GD CONNECT auf einem Arbeitsseminar zur Cloud-Sicherheit, das am 28.5.2013, kurz bevor Snowden an die Öffentlichkeit trat, abgehalten wurde, um die Warnungen des Verfassers zu erörtern.

[98] Europäischer Datenschutzbeauftragter (2013), Additional EDPS Comments on the Data Protection Reform Package.

[99] Europäischer Datenschutzbeauftragter (2011), Stellungnahme zur Mitteilung der Kommission – „Gesamtkonzept für den Datenschutz in der Europäischen Union“, Brüssel, 14. Januar 2011.

- eine Mindestquote bei den DSB von 25 % für technische Mitarbeiter mit geeigneten Qualifikationen (oder gleichwertiger Erfahrung) und der Möglichkeit des Aufstiegs[100] in Spitzenpositionen;

- Subventionen für den zivilgesellschaftlichen Sektor, obwohl sorgsam auf die Zweckbindung dieser Mittel geachtet werden muss. Die Verteilung der Mittel sollte gerecht und leistungsbezogen erfolgen, jedoch unter Vermeidung des lähmenden Effekts von Bürokratie und der Gefahr der institutionellen Bindung[101]. In den USA ermöglichen die Kultur der privaten Wohltätigkeit und eine die Massen mobilisierende Zivilgesellschaft vier hoch professionellen nationalen NRO[102], gestützt auf unterschiedliche Ansätze Rechtsstreitigkeiten zu Testfällen im Bereich Privatsphäre und Informationsfreiheit zu führen und erstklassige technische Kritiken zur Regierungspolitik zu erstellen. Demgegenüber gibt es in der EU noch immer einen Flickenteppich aus Dutzenden NRO, die infolge spärlicher Ressourcen und des Fehlens kontinuierlicher und fester personeller Forschungskapazitäten vor Snowdens Enthüllungen keine Kampagnen gegen FISA geführt haben.

[100] Die DSB wenden ein, sie seien nicht in der Lage, technische Mitarbeiter mit aktuellen Kenntnissen einzustellen oder an sich zu binden, da ihre Gehälter gegenüber denen des Privatsektors nicht konkurrenzfähig seien. Aufstiegschancen bei den DSB könnten einen hinreichenden Gleichstand bei der Vergütung zwischen technischen und juristischen Mitarbeitern bewirken, wodurch das Problem gemildert würde.

[101] Die „No Disconnect"-Strategie der EU etwa verpflichtet NRO, Berater für die Ausarbeitung formaler, bis ins kleinste Detail geregelter Ausschreibungsangebote zu engagieren, was kleine NRO ausschließt und nicht dem Geist der Zivilgesellschaft entspricht.

[102] Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), American Civil Liberties Union (ACLU) und Center for Democracy and Technology (CDT).

FAZIT

Wie bereits festgestellt, bestand einer der außergewöhnlichsten Aspekte der PRISM-Affäre darin, dass die Rechte von Nichtamerikanern nicht nur in den USA kein Diskussionsgegenstand waren, sondern sogar in den europäischen Medien erst lange nach den ersten Meldungen Beachtung fanden. Auf die Rechte von Nichtamerikanern wurde nur selten eingegangen, und bei einer flüchtigen Lektüre würde man nicht verstehen, dass Nichtamerikaner das beabsichtigte Ziel der Überwachung darstellten und keinerlei Rechte hatten.

Offenbar muss die einzige Lösung, die zur verlässlichen Beilegung der PRISM-Affäre geeignet ist, Änderungen des US-Rechts beinhalten, und dies sollte sich die EU zum strategischen Ziel setzen. **Ferner muss die EU mit großer Sorgfalt**[103] **prüfen, welches vertragliche Rechtsinstrument genau für eine künftige Einigung mit den USA vorzuschlagen ist**. Praktische[104], aber wirksame Mechanismen sind auch erforderlich, um zu sicherzustellen, dass Daten, die für gerechtfertigte strafrechtliche Ermittlungen an die USA weitergegeben werden, nicht missbraucht werden.

Bei der Bewertung der Auswirkungen der Enthüllungen und der Suche nach wirksamen Antworten sollten drei technische Überlegungen berücksichtigt werden:

(1) Daten können nur unverschlüsselt verarbeitet werden. Somit kann jeder Cloud-Verarbeiter nach FISA Abschnitt 702 insgeheim angewiesen werden, den Schlüssel oder die Informationen selbst unverschlüsselt auszuhändigen. Verschlüsselung ist zwecklos bei der Abwehr des Zugriffs der NSA auf die in US-Clouds verarbeiteten Daten (aber immer noch nützlich beim Schutz vor Angriffen von außen, etwa durch kriminelle Hacker). Die Nutzung der Cloud als ausgelagerte Festplatte bietet nicht die Wettbewerbs- und Größenvorteile der Cloud als Rechenmaschine („Compute engine"). **Das Problem lässt sich nicht technisch lösen**[105]**.**

(2) Bei einer Übertragung großer Datenmengen an ausgelagerte, der Überwachung unterliegende Cloud-Dienste wird Datenhoheit eingebüßt. Daher ist es vorzuziehen, die Daten in der EU zu belassen, solange keine rechtlichen Lösungen vorliegen. Obwohl die NSA über umfassende Kapazitäten für den gezielten Einsatz gegen bestimmte Systeme innerhalb der EU verfügt, ist dies schwerer und riskanter. Allerdings ist es erforderlich, die neue Verordnung grundlegend zu reformieren, sonst werden *in der Praxis* diese beiden Fälle als gleichwertig behandelt und Cloud-Aufträge an den kostengünstigsten Anbieter vergeben werden.

(3) Obwohl es bei einem in der EU ansässigen Unternehmen, das Geschäfte in den USA führt, auch zu einer Kollision zwischen dem EU-Datenschutzrecht und dem FISA-Gesetz kommen kann, ist es in der Praxis weniger wahrscheinlich, dass derartige geheime Anordnungen an das Unternehmen ergehen, da seine Rechtsabteilung und seine Unternehmensleitung wohl eher Widerstand leisten würden und als EU-Bürger weniger von

[103] Zu den „inhärenten" (aus seinem Amt abgeleiteten) Befugnissen des Präsidenten, die keiner Kongressvollmacht bedürfen, siehe: Fein, Bruce (2007), Presidential Authority to Gather Foreign Intelligence, Presidential Studies Quarterly, März 2007.

[104] Wills Aidan and al., Parliamentary Oversight of security and Intelligence Agencies in the EU, Studie für das Europäische Parlament, PE 453.207.

[105] Das exotische Verfahren der „homomorphen Verschlüsselung" wird bisweilen als Lösung vorgeschlagen, hat jedoch keine kommerzielle Relevanz, da es die Verarbeitung um ein Vielfaches verlangsamen würde und somit als systematisch eingesetzte Technik wettbewerbsuntauglich wäre.

den Spionagegesetzen der USA bedroht sind. „Clouds“ können Standortbeschränkungen unterworfen werden. Wer argumentiert, das Internet würde dadurch „balkanisiert“[106], verwechselt Fragen der Zensur mit dem Problem der Wahrung des privaten Charakters der Daten.

* * *

Die Gedankengänge, die die Enthüllungen Edward Snowdens in den Köpfen der Öffentlichkeit ausgelöst haben, lassen sich nicht rückgängig machen. Wir leben daher bereits in einer anderen Gesellschaft. Jeder weiß nun, dass die Geheimdienstgemeinschaft der USA möglicherweise alle persönlichen Geheimnisse kennt, die in Form elektronischer Daten in den Zugriffsbereich der NSA gesendet werden. Diese Entwicklungen könnten eine zutiefst destabilisierende Wirkung auf demokratische Gesellschaften haben, der Wahrnehmung grundlegender politischer Rechte und Menschenrechte entgegenstehen und eine neue Form einer augenblicklich verfügbaren und Zwang ausübenden panoptischen Macht entstehen lassen.

Zwischen den Verletzungen der Rechte von Amerikanern nach dem 4. Zusatzartikel und der Missachtung des Menschenrechts auf Schutz der Privatsphäre aller anderen Bewohner der Erde besteht eine historische Symmetrie. Im Vorfeld des US-amerikanischen Unabhängigkeitskriegs von 1776 führten die Briten anhand „allgemeiner Durchsuchungsbefehle“ genehmigte Durchsuchungen ohne Vorliegen eines Verdachts durch. Der Unmut[107] über diese Macht und ihren Missbrauch diente als Beweggrund für den späteren 4. Zusatzartikel zur US-Verfassung.

FISA Abschnitt 702 (oder*Paragraf 1881a*) bietet die Handhabe, mit einem allgemeinen Durchsuchungsbefehl Daten zu sammeln und die US-Außenpolitik betreffende Informationen abzuschöpfen, doch ist die Privatsphäre rechtlich (wenn auch theoretisch) unantastbar, es sei denn, die hohe gesetzliche Schwelle der „Notwendigkeit“ wird erreicht. Was die amerikanischen Revolutionäre so verärgerte, war ein zehn Jahre zurückliegender berühmter Fall des englischen Rechts[108], wonach solche allgemeinen Durchsuchungsbefehle verboten waren. Sie fanden es heuchlerisch, dass Gesetze, die sie nicht verfasst hatten und nicht ändern konnten, die Privatsphäre der kolonialen Herrscher, nicht jedoch die der kolonialen Untertanen schützten. Das gleiche Prinzip steht heute auf dem Spiel.

[106] US-Handelsministerium (Chefjustiziar) – Kerry, Cameron F. (2013), Grundsatzreferat beim German Marshall Fund of the United States, 28. August 2013.
[107] . https://www.eff.org/files/filenode/att/generalwarrantsmemo.pdf
[108] . Entick vs. Carrington 1765

LITERATURVERZEICHNIS

- ACLU FOIA request (2010), Introduction to FISA Section 702, (2010) Course Information, US Department of Justice, published December 2010
- Anzalda, Matthew A. and Gannon, Jonathan W. (2010), In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance (paywall), Texas Law Review, Vol 88:1599 2010
- ART29WP - Article 29 Data Protection Working Party (2012), Opinion on Cloud Computing, WP 196, Adopted July 1st 2012
- ART29WP - Article 29 Data Protection Working Party (2012), Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 195 Adopted on 6 June 2012
- ART29WP - Article 29 Data Protection Working Party (2013), Explanatory Document On The Processor Binding Corporate Rules, WP 204, Adopted On 19 April 2013
- Bigo Didier, Boulet Gertjan, Bowden Caspar, Carrera Sergio, Jeandesboz Julien, Scherrer Amandine (2012), Fighting cyber crime and protecting privacy in the cloud, Study for the European Parliament, PE 462.509
- Bloom, Stephanie Cooper (2009), What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform, Public Interest Law Journal Vol 18:269
- Bowden, Caspar (2011), Government Databases and Cloud Computing (slides), The Public Voice, Mexico, October 2011
- Bowden, Caspar (2012), Is EU data safe in US Clouds? (slides), *Academy* of European Law, Trier September 2012
- Cloud, Morgan (2005), A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment, Ohio State Journal of Criminal Law, Vol 3:33 2005
- Cole, David, (2003), Georgetown Law: The Scholarly Commons, Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens? 25 T. Jefferson L. Rev. 367-388
- Congressional Research Service - Bazan, Elizabeth B. (2008), The Foreign Intelligence Surveillance Act: An Overview of Selected Issues, Updated July 7, 2008, RL34279
- Congressional Research Service – Liu, Edward C. (2013), Reauthorizattion of the FISA Amendments Act, 7-5700, R42725, January 2, 2013
- Congressional Research Service (2007), P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, August 23, 2007
- Corradino, Elizabeth A. (1989), Fordham Law Review, The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far? Volume 57, Issue 4, Article 4, January, 1989
- De Filippi, Primavera, and McCarthy, Smari (2012), Cloud Computing: Centralization and Data Sovereignty, European Journal of Law and Technology 3, 2
- Desai, Anuj C. (2007), Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy, Stanford Law Review, 60 STAN L. REV. 553
- Dhont J., Asinari M.V.P., Poullet Y., Reidenberg J., Bygrave L. (2004), Safe Harbour Decision Implementation Study, European Commission, Internal Market DG Contract PRS/2003/A0-7002/E/27
- Dulles, Allen Welsh (1963), The Craft of Intelligence, New York: Harper&Row.

- European Commission (2011), [Draft] Proposal for a General Data Protection Regulation
- European Commission (2012), Proposal for a General Data Protection Regulation, 25.1.2012, COM(2012) 11 final 2012/0011
- European Commissioner - Reding, Viviane (2013), Letter to the Attorney General, Ref. Ares (2013)1935546 - 10/06/2013, Brussels, 10 June 2013
- European Data Protection Supervisor - Hustinx, Peter (2010), Data Protection and Cloud Computing Under EU Law, speech, Third European Cyber Security Awareness Day, BSA, European Parliament, 13 April 2010, Panel IV: Privacy and Cloud Computing
- European Data Protection Supervisor (2011), Opinion on the Communication - "A comprehensive approach on personal data protection in the European Union", Brussels, 14 January 2011
- European Data Protection Supervisor (2013), Additional EDPS Comments on the Data Protection Reform Package
- Fein, Bruce (2007), Presidential Authority to Gather Foreign Intelligence, Presidential Studies Quarterly, March 2007
- Forgang, Jonathan D. (2009), "The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas, Fordham Law Review, Volume 78, Issue 1, Article 6, 2009
- Hoboken, J.V.J., Arnbak, A.M., Van Eijk, N.A.N.M (2012), Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act, IVIR, Institute for Information Law, University of Amsterdam, November 2012 (English Translation)
- Hon, W. Kuan and Millard, Christopher (2012), Data Export in Cloud Computing - How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4, QMUL Cloud Legal Project, 4 April 2012
- Hondius, Frits W (1975), Emerging data protection in Europe. North-Holland Pub. Co.
- International Working Group on Data Protection in Telecommunications (2012), Working Paper on Cloud Computing - Privacy and data protection issues - Sopot Memorandum, 51st meeting, 23-24 April 2012
- Kuner, Christopher, (2008), Membership of the US Safe Harbor Program by Data Processors, The Center For Information Policy Leadership, Hunton & Williams LLP
- LoConte, Jessica (2010), FISA Amendments Act 2008: Protecting Americans by Monitoring International Communications--Is It Reasonable?, Pace International Law Review Online Companion 1-1-2010
- Medina, M. Isabel, (2008) Indiana Law Journal, Exploring the Use of the Word "Citizen" in Writings on the Fourth Amendment Volume 83, Issue 4, Article 14, January, 2008
- Pell, Stephanie K. (2012), Systematic government access to private-sector data in the United States, International Data Privacy Law, 2012, Vol. 2, No. 4
- Radsan, John A. (2007), The Unresolved Equation of Espionage and International Law, Michigan Journal of International Law, Vol 28:595 2007
- Snider, Britt L. (1999): Unlucky SHAMROCK - Recollections from the Church Committee's Investigation of NSA
- U.S. Ambassador to the EU (2012), Remarks by William E Kennard, Forum Europe's 3rd Annual European Data Protection and Privacy Conference, December 4, 2012
- U.S. Commerce Department (General Counsel) – Kerry, Cameron F. (2013),

Keynote Address at the German Marshall Fund of the United States, 28th August 2013

- US Congress (2008), Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 122 Stat. 2436, Public Law 110-261, July 10, 2008
- US Department of Commerce International Trade Administration (2013), Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing, December 4, 2012
- US State Department (2012), Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the EU and the US
- Vandekerchkhove, Wim (2010), European whistleblower protection: tiers or tears?, in D. Lewis (ed) A Global Approach to Public Interest Disclosure, Cheltenham/Northampton MA, Edward Elgar, pp 15-35.
- Walden, Ian (2011), Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, QMUL Cloud Legal Project, Research Paper No. 74/2011
- Weichert, Thilo (2011), Cloud Computing and Data Privacy, The Sedona Group Conference Working Group Series, February 2011
- Wills Aidan, Vermeulen Mathias, Born Hans, Scheinin Martin, Wiebusch Micha, Thornton Ashley, Parliamentary Oversight of security and Intelligence Agencies in the EU, Note for the European Parliament, PE 453.207.
- Young, Stewart M, (2003) Michigan Telecommunications and Technology Law Review, Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases, Volume 10, Rev. 139

EUROPÄISCHES PARLAMENT

CATALOGUE BA-02-13-390-DE-C

GENERALDIREKTION INTERNE POLITIKBEREICHE

FACHABTEILUNG C
BÜRGERRECHTE UND KONSTITUTIONELLE ANGELEGENHEITEN

Rolle

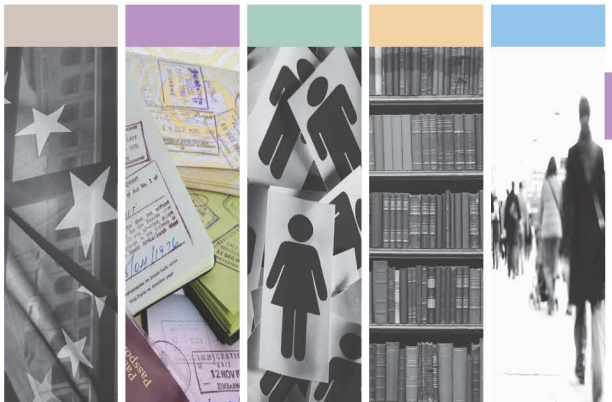
Die Fachabteilungen sind Forschungsreferate, die Ausschüsse, interparlamentarische Delegationen und andere parlamentarische Einrichtungen beraten.

Politikbereiche

- Konstitutionelle Fragen
- Freiheit, Sicherheit und Justiz
- Gleichstellung der Geschlechter
- Rechts- und Parlamentarische Angelegenheiten
- Petitionen

Dokumente

Siehe Website des Europäischen Parlaments:
http://www.europarl.europa.eu/studies



ISBN 978-92-823-5061-4
doi: 10.2861/31404

Amt für Veröffentlichungen