Dr. Dr. h.c. Burkhard Hirsch

40545 Düsseldorf
Rheinallee 120
Tel.: 0211 - 55 13 31
Fax: 0211 - 55 37 03
im April 2014

**Bemerkungen in einem Symposium der BRAK
Zur anwaltlichen Verschwiegenheit und dem NSA – Skandal
am 9.5.2014 in Berlin.**

Der NSA – Skandal ergibt sich aus drei unterschiedlichen Elementen, nämlich

- aus der jahrelang verdrängten Erkenntnis, dass die modernen Fähigkeiten der sich dramatisch entwickelnden IT – Technologie nicht nur zu einem Zuwachs der persönlichen und wirtschaftlichen Kommunikation mit elektronischen Mitteln geführt hat, sondern auch zu einer massiven Gefährdung der Privatheit, der Freiheit und des Schutzes der Kommunikation vor staatlicher und privater Überwachung,

- aus der wachsenden Verflechtung deutscher, europäischer und US-amerikanischer Datenübermittlung aus wirtschaftlichen und politischen Gründen, die sich ohne Rücksicht auf die elementaren Unterschiede in der rechtlichen Bewertung des Datenschutzes ergeben hat, und

- aus dem nur schrittweise und unvollständig bekannt werdenden Umfang nachrichtendienstlicher Tätigkeiten der National Security Agency (NSA) und in gleicher Weise des britischen Government Communications Headquater (GCHQ) einschließlich ihrer Zusammenarbeit mit dem BND, die nur schrittweise aus den Veröffentlichungen des Edward Snowden und seiner journalistischen Helfer bekannt werden.
  Dazu gehören insbesondere bei der NSA der direkte Zugriff auf die zentralen Server der führenden US-Internetkonzerne (PRISM-Programm), das Anzapfen von Kabeln (Upstream), die Analyse von Inhalts- und Verbindungsdaten (XKeyscore), die Umgehung von Verschlüsselungen im Internet (BullRun-Programm), der Zugang zu Telefon- und Standortdaten, und beim GCHQ die Überwachung der transatlantischen Glasfaserkabel (Tempora-Programm), das Entschlüsselungsprogramm Edgehill, Programme für Informationssysteme (Quantumtheory und Foxacid) und das Programm für die Speicherung von täglich 200 Mio SMS-Textnachrichten (Dishfire - Programm).[1]

[1] vgl. dazu den Beschluss des Europ.Parlaments v. 12. 3. 2014, zum „Überwachungsprogramm der NSA, Überwachungseinrichtungen in mehreren Mitgliedsstaaten und Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres".
(Aktz. 2013/2188 INI; A 7-0139/2014); Ergebnisse Zif. 2

Die Bundesregierung hat detaillierte parlamentarische Anfragen zu diesen Komplexen nur sehr zögernd und lustlos unter Berufung auf übergeordnete und geheimhaltungsbedürftige Interessen der Bundesrepublik beantwortet.[2]

Bemerkenswerter sind der sog. Bowden-Bericht der EU-Generaldirektion Interne Politikbereiche „Die Überwachungsprogramme der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger" v. Sept. 2013, die Mitteilung der Kommission an das EU-Parlament über die Funktionsweise der Safe-Harbour-Regelung v. 27. 11. 2013, der Bericht der Vorsitzenden einer EU-Arbeitsgruppe zum Datenschutz v. 27. 11. 2013, die Unterrichtung des BfDI über Abhöraktivitäten US-amerikanischer Nachrichtendienste in Deutschland v. 15. 11. 2013 [3] sowie sein 24. Tätigkeitsbericht [4]– und schließlich der eindrucksvolle Beschluss des Europäischen Parlamentes v. 12. 3. 2014 zum „Überwachungsprogramm der NSA, Überwachungseinrichtungen in mehreren Mitgliedsstaaten und Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres" [5]

Der Beschluß schließt mit 133 Ergebnissen und Empfehlungen ab und ist von außerordentlicher Bedeutung und bedarf einer besonderen Würdigung. Er verurteilt ohne Umschweife die massenhafte Überwachung und Speicherung von Daten zahlloser Bürger ohne konkreten Anlass und ohne Möglichkeit konkreter Rechtsmittel als einen Verstoß gegen grundlegende Prinzipien einer freien Gesellschaft, der auch nicht mit dem Kampf gegen Terrorismus begründet oder gerechtfertigt werden kann. Er fordert die unverzügliche Suspendierung der sog. Safe-Harbour-Regelung und der verschiedenen gemeinsamen Datenverarbeitungsprogramme zwischen der EU und den USA über Passagierlisten oder Finanzbewegungen. Er prangert das Anzapfen der umfangreichen Datensammlungen an, die von den in den USA ansässigen Betreibern sozialer Netzwerke unterhalten werden. Er fordert die Kommission und die Mitgliedstaaten der EU auf, das geplante Freihandelsabkommen mit den USA[6] nur dann abzuschließen, wenn die pauschale Massenüberwachung und das Abfangen von Nachrichten in EU-Institutionen und diplomatischen Vertretungen völlig eingestellt worden sind.
Das Europäische Parlament werde dem endgültigen TTIP-Abkommen nur zustimmen, wenn u.a. die von der EU—GRCh anerkannten Grundsätze in vollem Umfang respektiert werden und der Schutz der Privatsphäre des Einzelnen gesichert sei. Er fordert von den EU-Staaten die Solidarität gemeinsamen Handelns. Er lehnt Sonderabkommen zwischen einzelnen EU-Staaten und den USA als eine Gefährdung dieser Solidarität ab und behält sich vor, diese bisher angestrebten Sonderverträge auf ihre Vereinbarkeit mit den europarechtlichen Pflichten der Mitgliedstaaten zu prüfen und ggfls. zu sanktionieren.
Der Beschluss bezieht sich auch mehrfach auf die besondere rechtsstaatliche Bedeutung der Berufsgeheimnisse zwischen Anwalt und Mandanten oder für die Pressefrei-

---

[2] vgl. BtDrS. 17/14560 v. 14. 8. 2013 und 17 / 14602 v. 22. 8. 2013.
[3] BtDrS. 18 / 59
[4] f. d. Jahre 2011/ 2012 insbes. zu TZr. 2.5.1 SWIFT-Daten, 2.5.2 zu PNR und 5.3. zu Cloud Computing
[5] vgl. oben Anm. 1
[6] Abkommen über die transatlantische Handels- und Investitionspartnerschaft (TTIP), vgl. Beschluss a.a.O. Empfehlungen 73, 74

heit und fordert einen besonderen Schutz der Whistleblower und der in der NSA – Affäre tätig gewordenen Journalisten vor politischer Verfolgung.
Dieser Beschluss unterscheidet sich eindrucksvoll von allen bisherigen vorsichtig gewundenen Erklärungen der Kommission und auch – wie man leider feststellen muss - der Bundesregierung. Er schließt mit einem aus 8 Aktionen bestehenden „europäischen digitalen habeas corpus Grundsatz – Schutz der Grundrechte in einem digitalen Zeitalter", der jede Unterstützung verdient.

Es ist bemerkenswert, dass diese Berichte und der geschilderte Beschluss des Europäischen Parlamentes in der deutschen Presse kaum erölrtert wurden und in der Politik der Bundesregierung bisher überhaupt keinen Niederschlag gefunden haben, während die einschlägige Fachliteratur auch durch Autoren aus international tätigen Praxen langsam Fahrt aufnimmt.[7]

1. Es braucht hier nicht weiter begründet zu werden, dass die Freiheit der nationalen und internationalen Telekommunikation nicht nur ökonomische Bedeutung hat, sondern dass die Gewährleistung ihrer Sicherheit und Integrität ein wesentliches, von dem Grundgesetz garantiertes Freiheitselement ist. Auch der Kampf gegen den Terrorismus darf nicht dazu führen, dass rechtsstaatliche Grundelemente aufgegeben werden, ganz abgesehen davon, dass ohnehin einzelne bekannt gewordene Vorgänge nun wirklich mit dem Kampf gegen Terrorismus nicht begründet werden können, wie das Abhören des Handys der Kanzlerin oder das Abhören von Sekretariaten und Botschaften der Europäischen Union.

Auch das Urteil des EuGH v. 8. 4. 2014 zur Vorratsdatenspeicherung[8] betont die entscheidende Bedeutung der freien und nicht überwachten Kommunikation für die Rechtsstaatlichkeit unserer Rechtsordnung - übrigens verbunden mit der Erwägung, dass die Vorratsspeicherung von Verbindungsdaten nur bei solchen Personen vorgenommen waren sollte, von denen eine Nähe zu den zu bekämpfenden Straftaten angenommen werden kann.
Die Kommunikation von Berufsgeheimnisträgern, wie die Kommunikation des Anwalts mit seinem Mandanten, sollte, wie das nach diesem für das europäische Verfassungsrecht verbindlichen Urteil ausdrücklich erklärt, von einer Vorratsspeicherung der Verkehrsdaten ausgenommen werden.

2. Im Laufe des Kalten Krieges wurden auch in der Bundesrepublik von den amerikanischen militärischen Einheiten Abhöreinrichtungen errichtet, von denen insbesondere die Echelon – Affäre mit Einrichtungen in Bad Aibling bekannt wurde. Die dortigen Einrichtungen bezogen sich auf das Abhören von Satelliten. Es wird wohl zutreffend angenommen, dass nicht nur militärisch bedeutsame, sondern auch wirtschaftlich interessierende Informationen erhoben wurden. Eine exakte Aufklärung, die

---

[7] vgl. etwa Becker/Nikolaeva, Das Dilemma der Cloud-Anbieter zwischen USPatriotAct und BDSG. CR 3/2012, S. 170 ff; Gärditz, Stuckenberg, Vorratsdatenspeicherung a la americaine, JZ 2014, 209 ff; Ewer, Thienel, Völker-, unions- und verfassungsrechtl. Aspekte des NSA-Datenskandals, NJW 2014, 30ff.; Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsstrukturen, JZ 2014, 53 ff.
[8] Rechtssachen C-293/12 und C-594/12 Digital Rights Ireland und Seitlinger u.a. v. 8. 4. 14

auch vom EU-Parlament verlangt wurde, unterblieb infolge des Attentates von 11. 9. 2001 und die Übernahme der Einrichtung durch den BND.

Zunächst waren den damaligen alliierten Besatzungstruppen durch nicht veröffentlichte Verwaltungsabkommen eigene Abhörrechte in der Bundesrepublik zugestanden worden. Sie sind allerdings sämtlich mit der Wiedervereinigung und spätestens mit übereinstimmenden Erklärungen im August 2013 nochmals aufgehoben worden.
Es ist nicht mehr ernsthaft streitig, dass es damit keine irgendwie gearteten deutschen Rechtsgrundlagen für eigene heimliche Datenerhebungen der in der Bundesrepublik stationieren ausländischen NATO-Streitkräfte oder der ihnen zugeordneter privaten Gesellschaften mehr gibt.

3. Für die unberechtigte Erhebung von Daten durch die NSA in der Bundesrepublik oder der GCHQ sind zahlreiche und erhebliche Strafbestimmungen einschlägig, so die §§ 201 bis 206 und 99 StGB. Der Generalbundesanwalt hat dazu ein sog. Beobachtungsverfahren eingeleitet, eine Vorstufe strafrechtlicher Ermittlungen.
Aber gegen wen sollen sie sich richten ?

Nach deutschem Recht können sich nur natürliche Personen strafbar machen. Soweit es sich um Botschaftsangehörige handelt, genießen sie diplomatische Immunität, auch soweit sie durch nachrichtendienstliche Tätigkeit gegen die Wiener Konvention verstoßen. Sie können nur –und sollten dann allerdings auch - nach Hause geschickt werden.

Man muss davon ausgehen, dass die denkbaren strafrechtlich relevanten Straftaten überwiegend im Ausland begangen werden. Das ist zwar für den Tatbestand des § 99 StGB für die Anwendung des deutschen Strafrechts gem. § 5 Zif. 4 StGB rechtlich ohne Bedeutung, für die Straftaten des § 201 ff StGB jedoch nicht. Es würde zwar nach § 9 StGB ausreichen, dass rechtswidrig aufgenommene Daten in Deutschland aufgenommen oder verarbeitet wurden, bei einer reinen Auslandstat kommt die Anwendung deutschen Strafrechts aber nach § 5 StGB nur in Betracht, wenn sich die Tat gegen einen Deutschen richtet und auch am Tatort mit Strafe bedroht ist. Diese Voraussetzung liegt jedenfalls in den Vereinigten Staaten nicht vor, wie noch dargestellt werden wird.

Wir werden also auf den Generalbundesanwalt nur beschränkte Erwartungen setzen können.

4. Größere Erwartungen werden in der Bundesrepublik – schon aus allgemeinen politischen Gründen - auf den Abschluss eines sog. No-Spy-Abkommens mit den USA gesetzt. Dabei wird an das Vorbild der sog. Big Five gedacht, also an Absprachen zwischen den USA, Kanada, Großbritannien, Australien und Neuseeland. Diese Absprachen haben ihre Wurzeln in der Zusammenarbeit im Zweiten Weltkrieg und enthalten keinen völkerrechtlich formell verbindlichen Verzicht auf Spionage, sondern nur allgemeine Freundschaftsbekundungen. Die Vereinigten Staaten haben

jedenfalls weder ein Vorbild, noch ein erkennbares Interesse an einem völkerrechtlich verbindlichen, mit Sanktionen belegten Abkommen über einen Spionageverzicht.
Auch das Europäische Parlament hat sich ausdrücklich gegen ein separates Abkommen einzelner Mitgliedstaaten als einen Bruch der notwendigen Solidarität gegenüber einem Verhalten ausgesprochen, das alle europäischen Bürger in gleicher Weise trifft, und darum dringend ein gemeinsames Verhalten der EU und ihrer Mitgliedsstaaten gefordert.[9]
Die Erwartung eines separaten No-Spy-Abkommens ist eine Illusion, die man aufgeben sollte.

5. Weitgehende Übereinstimmung besteht darin, dass die Bundesregierung verpflichtet ist, die Grundrechte der deutschen Bürger gegen ihre Verletzung auch durch internationale Aktivitäten zu schützen. Das BVerfG hat die Bundesregierung in seiner Entscheidung zur Vorratsdatenspeicherung dazu ausdrücklich aufgefordert.[10] Allerdings räumt die Rechtsprechung der Regierung dazu einen breiten Ermessensspielraum ein, was sie dazu tatsächlich tun sollte. Auch das Europäische Parlament hat in seinem bereits erwähnten Beschluss v 12. 3. 2014 die Mitgliedsstaaten wiederholt dazu aufgefordert, die Pflicht zum Schutz ihrer Bürger zu erfüllen.[11]

Die Bundesregierung hat gemeinsam mit Brasilien einen Vorstoß bei den UN zum Internationalen Pakt über bürgerliche und politische Rechte (IPbpR) von 1966 unternommen. Beschlüsse der Generalversammlung der UN dazu haben aber nur empfehlende Bedeutung und es ist nicht unstreitig, ob der Pakt nur die Rechte im eigenen Land meint oder auch Ansprüche gegen Handlungen begründet, die von einem anderen Land ausgehen.[12]
Es käme auch in Betracht, die (noch nie angewendete) Staatenbeschwerde zum UN-Menschenrechtsausschuss – die nur in Empfehlungen mündet - durch ein Individualbeschwerderecht zu ergänzen. Zur Durchsetzung solcher Beschwerden könnte dann der IGH angerufen werden.[13]

Allerdings haben sich bisher weder die USA noch Großbritannien dem Individualbeschwerdeverfahren zum IPbpR unterworfen. Im übrigen hat sich die USA der Zuständigkeit des Internationalen Gerichtshofs in den Haag (IGH) ohnehin nicht generell unterstellt, sondern sich nur ihre fallweise Anerkennung vorbehalten.

Demgegenüber unterliegt Großbritannien den Verpflichtungen aus der EMRK und dem Recht der EU.
Nach dem sog. TEMPORA-Programm des GCHQ wird die Überwachung innerstaatlicher Datenströme nur an eine einschränkende ministerielle Anordnung gebunden, die außerdem nicht für Datenströme gilt, die außerhalb des Vereinigten Königreichs ge-

---

[9] vgl. oben Anm. 1, Empfehlungen 123, 124.
[10] vgl. BVerfGE 125,260 v. 2.3.10, Rdzf. 218. Vgl. zu dieser verfassungrechtlichen Schutzpflicht besonders eindringlich Hoffmann-Riem, a.a.O. S. 56 ff.
[11] vgl. Beschluss (Anm. 1),Empfehlungen 20 ff.
[12] vgl. Ewer,Thienel, a.a.O. S.32
[13] vgl. Schmahl, „Effektiver Rechtsschutz gegen Überwachungsmaßnahmen ausländischer Geheimdienste ?" JZ 2014, 220 ff (222)

sendet oder empfangen werden. Die Bedingungen der Art. 8, 10 EMRK werden damit verletzt.[14] Denn nach ständiger Rechtsprechung des EGMR müssen für Überwachungsmaßnahmen die Straftaten, die betroffenen Personengruppen, die zeitliche Begrenzung, die Regelung der weiteren Verwendung und Verarbeitung, der Schutz vor Missbrauch und die Umstände gesetzlich geregelt sein, nach denen die Löschung der Daten und die Vernichtung der Bänder erfolgt. Die Maßnahme muss durch eine unabhängige Institution angeordnet werden und der Betroffene muss nach ihrer Erledigung die Möglichkeit der richterlichen Überprüfung haben.[15] Diese Voraussetzungen werden bei dem TEMPORA-Programm nicht erfüllt.

Im Übrigen hat Großbritannien zwar für sich die Anerkennung der EU GRCh ausdrücklich ausgeschlossen[16]. Doch ist der Art. 8 GRCh auch in Art. 16 Abs. 1 AEUV enthalten. Es bleibt jedoch die offene Frage, ob Großbritannien mit dem Tempora – Programm ausschließlich Rechte der nationalen Sicherheit ausübt, wozu es europarechtlich berechtigt ist.[17]

Gleichwohl könnte und sollte die Bundesregierung zumindest darauf dringen, dass die bestehende Praxis mi dem Geist der Verträge unvereinbar ist und jedenfalls europäische Kommunikationsteilnehmer nicht anders behandelt werden dürften, als britische Staatsangehörige.

6. Aus all dem folgt, dass wir auf ein gemeinsames europäisches Vorgehen angewiesen sein werden. Dazu muss zunächst die Frage behandelt werden, welche Auswirkungen das nationale US-amerikanische Recht auf die Abkommen hat, die mit der EU geschlossen wurden.

a. Der grundlegendste Unterschied besteht zunächst darin, dass der Schutz der persönlichen Daten nach dem 4. Amendment zur amerikanischen Verfassung nur amerikanischen Staatsangehörigen, in gewissem Umfang auch ständigen Residenten in den USA[18] zusteht. Im Gegensatz zum deutschen Recht steht Ausländern grundsätzlich kein Datenschutz zu.
Technisch werden nicht nur die von den USA ausgehenden oder dorthin führende Kommunikationen, sondern auch Kommunikationen zwischen Ausländern erfasst, die außerhalb der USA stattfinden.
Das geschieht dadurch, dass von den Providern alle Arten der Telekommunikation nach der Kapazität und den Kosten über die jeweils vorhandenen Server geführt werden – wo immer die sich befinden mögen -, sodass z. B. auch ein deutsches Inlandsgespräch über einen Server in den USA gesteuert werden und – nach amerikanischem Recht – dort nachrichtendienstlich erfasst und gespeichert werden kann. Es gibt die Möglichkeit, die transatlantischen Kabel zu überwachen oder die Zusammenarbeit der Nachrichtendienste zu nutzen. So hat der BND in Afghanistan geführte Telefonate im

---

[14] EGMR –Urteil v.29. 6.2006, NJW 07, S. 1433 ff
[15] vgl. Schmahl, a.a.O. S.225 u.d.d.Zit.
[16] ABl.EU 2010, Nr. C 83, 313. Schmahl a.a.O., S. 223
[17] vgl. Ewert, Thienel, a.a.O. S.33
[18] Personen, die nicht nur einen festen Wohnsitz in den USA haben, sondern zu dem Land erkennbar feste ständige Beziehungen geknüpft haben.

Wege der Auslandsaufklärung „im offenen Himmel“ außerordentlich umfangreich erfasst und der NSA übermittelt – soweit ich sehe, ohne eine dafür nach deutschem Recht erforderliche Rechtsgrundlage, da die Rechte aus Art. 10 GG nicht nur deutschen Staatsangehörigen, sondern jedermann zustehen.[19]

b. Die NSA kann im Rahmen des sog. PRISM- Programms auch die in den USA tätigen IT-Gesellschaften verpflichten, der NSA alle denkbaren Daten der Telekommunikation und Datenspeicherung zu übermitteln. Sie erstreckt diese Möglichkeit auch auf in Europa tätige Filialen oder Tochtergesellschaften der einschlägigen Gesellschaften und der großen in den USA domizilierenden Sozialnetzwerke. [20] Das erfolgt auch, wenn es sich um eine in den USA tätige amerikanische Tochter eines deutschen Unternehmens handelt. Es kommt dabei auch nicht darauf an, ob eine konzernrechtliche Verbindung besteht, es genügt eine wesentliche finanzielle Verflechtung.

Die NSA berücksichtigt nicht, ob ihre Forderung gegen das europäische oder das jeweilige Datenschutzrecht des Landes verstößt, in dem die Mutter oder die Tochter ihren Sitz hat. Denn die NSA selbst handelt ja nur in den Vereinigten Staaten.

Eine Verweigerung der Datenherausgabe wird mit Bußen belegt und kann z. B. in Fällen, in denen eine Order des FISC vorliegt, als contempt of court geahndet werden. Die einschlägigen Gesellschaften können also wählen, ob sie nach dem nationalen Recht ihres Konzerns oder nach europäischem Recht bebußt werden wollen. Die Vermutung liegt nahe, dass sie eher die Verletzung des europäischen Rechts riskieren, weil die Gefahr, ertappt zu werden, relativ gering ist und die ggfls. hier zu zahlenden Bußen erheblich niedriger sind, als die rechtlichen und ökonomischen Folgen in den Vereinigten Staaten.

Schließlich ist es kein Geheimnis, dass die transatlantischen Glasfaserkabel an ihren jeweiligen Landestellen in den USA oder in England - dort mit dem Tempora-Programm - angezapft werden.

c. Für amerikanische Staatsbürger gibt es nach bisheriger Rechtsprechung - die sich langsam zu wandeln scheint – kein Schutz vor der Speicherung sog. Meta-Daten, also für Daten, die der Betroffene einem Dritten offenbart hat. Dazu gehören Verbindungsdaten aller Arten der elektronischen Kommunikation, aber auch Kreditkarten, Kontonummern usw. Sie fallen nicht unter das 4. Amendment. Diese Daten können ohne Beschränkung gespeichert werden, was in der Regel auf 5 Jahre geschehen soll.
Im Fall einer rechtlich genehmigten Recherche erfolgt die Datenauswertung in 3 Gruppen in einer Art Schneeballsystem. Die erste Gruppe umfasst sämtliche Telekommunikationskontakte, die die interessierende Person in den letzten 5 Jahren gehabt hat. Die zweite Gruppe erfasst alle Kontakte von Mitgliedern der ersten Gruppe in den letzen 5 Jahren mit anderen Personen. Die dritte Gruppe erfasst alle Telekommunikati-

---

[19] vgl. Petri, Déjà vu – datenschutzpolitische Aufarbeitung der PRISM-Affäre. Appell nach mehr Transparenz der nachrichtendienstlichen Tätigkeit. ZD 2013, 557 ff; Huber,Die strategische Rasterfahndung des BND – Eingriffsbefugnisse und Regelungsdefizite. NJW 2013, 2572 ff.

[20] In diesem Zusammenhang wurden in publizierten vertraulichen Dokumenten Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype und You Tube genannt, jedoch nicht offiziell bestätigt. Einzelne Anbieter sollen ihre Daten -Übermittlungen in die USA bewusst nicht verschlüsselt haben.

onskontakte der Mitglieder der zweiten Gruppe, die diese Mitglieder in den letzten Jahren gehabt hatten – was zu einer ungeheuren Vielzahl führen kann.

d. Formell ist der Zugriff auf sog. Meta-Daten oder inhaltliche Nachforschungen möglich durch präsidentielle Entscheidung (Executive Order 12333) oder nach Sect. 702 FISA (Foreign Intelligence Surveillance Act) bzw. nach Sect. 215 US Patriot Act unter leichten Begrenzungen.

Es genügt die auf Einzelpersonen oder Gruppen bezogene Entscheidung des FISC (Foreign Intelligence Surveillance Court), die jährlich erneuert wird, geheim ist und bleibt und deren Voraussetzungen ständig erweitert wurden. Es genügt ein recht loser Zusammenhang mit Ermittlungen nachrichtendienstlicher Tätigkeiten oder mit der wünschenswerten Aufklärung nationaler politischer Interessen. Eine Benachrichtigung der Betroffenen oder eine Löschung der gespeicherten Daten nach bestimmter Zeit ist nicht vorgesehen.

Die Exaktheit der Voraussetzungen und die Bewertung der Entscheidungen des FISC sind schon deswegen sehr unterschiedlich, weil nach amerikanischem Recht die Speicherung von Daten i.d.R. noch nicht als Verletzung von Datenschutzrechten gilt, sondern erst ihre individuelle Auswertung. Bei offiziellen Verhandlungen einer EU – US Working Group on Data protection haben im übrigen die Vertreter der US alle detaillierten Auskünfte über exakte Bedingungen oder die Zahl der betroffener Personen ausdrücklich abgelehnt.[21]

Der Bericht kommt zu dem Ergebnis, dass die Zahl der betroffenen europäischen Bürger und der Umfang der über sie gesammelten Daten unklar geblieben ist. Während die Erhebung der Daten von US-Bürgern für die Ermittlungen über geheimdienstliche oder terroristische Tätigkeiten „notwendig" sein muss, gilt das für Daten von Europäern nicht. Es genügt ein möglicher Sachzusammenhang. Es gibt dazu keine spezifischen Vorschriften, nach denen die Sammlung, Verarbeitung oder Speicherung ihrer Daten auf das Notwendige beschränkt werden muss, selbst wenn sie keine Verbindung zu Spionage, Terrorismus, kriminelle, rechtswidrige oder gefahrtragende Tätigkeiten haben.
Irgendwelche Rechtsmittel sind nicht gegeben.
„Da Anordnungen des FISC geheim und die Gesellschaften zur Geheimhaltung verpflichtet sind, in welchem Umfang sie zur Mitwirkung verpflichtet wurden, sind keine rechtlichen oder administrativen Möglichkeiten für EU oder US Betroffene gegeben, etwas darüber zu erfahren, ob ihre persönlichen Daten gespeichert oder weiter verarbeitet werden. Es gibt für Einzelpersonen keine Möglichkeit, Zugang zu ihren Daten, Berichtigung oder Löschung zu erlangen oder eine verwaltungsmäßige oder richterliche Kontrolle zu erwirken."[22]

---

[21] vgl. Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection v. 27. Nov. 2013. Es wird geschätzt, dass die NSA zur Zeit etwa 170.000 Personen überwacht.
[22] vgl. Report , Zif. 5: Summary on Main Findings.

e. Von erheblicher praktischer Bedeutung ist die Frage, ob sich die Vereinigten Staaten an die Abkommen[23] gehalten haben, die mit ihnen hinsichtlich der Flugpassagierdaten (PNR) [24], hinsichtlich verdächtiger Finanzbewegungen über Bankkonten (TFTP)[25], sowie zu den Zahlungsverkehrsdaten SWIFT [26] getroffen worden sind.
Die einschlägigen US-Regierungsstellen haben zwar versichert, dass die Bedingungen dieser Abkommen von den dafür zuständigen Stellen beachtet worden sind. Sie haben aber ausdrücklich die Beantwortung der Fragen der EU – Vertreter verweigert, ob amerikanische Behörden auf andere Weise Zugang zu den Daten bekommen haben.
Der Bericht kommt zu der dringenden Empfehlung, nicht nur das Europäische Datenschutzrecht unverzüglich zu vereinheitlichen und zu modernisieren, sondern von den amerikanischen Partnern klare Rechtsregeln, justitiable Rechtsbehelfe und Kontrollen und eine „Schutzschirm"-Regelung zu verlangen, die die Rechte von Amerikanern und Europäern sichert, um die im beiderseitigen Interesse liegenden Schutzmechanismen zu erhalten und weiterzuentwickeln.[27]

f. Von zumindest ebenso großer Bedeutung ist die Behandlung der sog. Safe-Harbour-Regelung.[28] Wenn amerikanische Unternehmen vom dortigen Handelsministerium als Gesellschaften registriert worden sind, die den Safe-Harbour-Regeln entsprechen, dann können ihnen Daten aller Art wie an inländische Unternehmen übermittelt werden.

Voraussetzung ist eine Selbst-Zertifizierung der als Safe-Harbour z. Zt. 3246 registrierten Unternehmen, dass es in seinen Geschäftsbedingungen kompatible Datenschutzbestimmungen vereinbart, die es veröffentlicht hat und in denen u. a. dem jeweiligen Geschäftspartner auch das freie Wahlrecht eingeräumt wird, ob er mit einer Weiterübermittlung seiner Daten einverstanden ist oder nicht. Es steht fest, dass ein erheblicher Teil der als Safe-Harbour registrierten Unternehmen diese Voraussetzung nicht erfüllt, ohne dafür gerügt worden zu sein. Im Übrigen hat sich ergeben, dass etwa 10 % der Unternehmen, die sich als zertifiziert bezeichnet haben, das in Wirklichkeit nicht oder nicht mehr sind. Soweit sie in den Listen als „not current" bezeichnet werden, gelten die Verpflichtungen nur für früher gespeicherte Daten.
Über die Hälfte der als Safe Harbour registrierten Unternehmen verarbeiten Daten von Mitarbeitern in Europa, die zu personaltechnischen Zwecken in die USA übermittelt wurden.

Diese Safe-Harbour-Regelung ist für das sog. Cloud Computing entscheidend, also für die kostengünstige Auslagerung der Speicherung, Verarbeitung und Übermittlung ver-

---

[23] vgl. Communication f. the Commission to the European Parliament and the Council "Rebuilding trust in EU-US data flows Aktz. Com(2013)846;
vgl. auch Beschluß des Europ.Parlam. v.12. 3. 2014 (oben Anm.1) TxtZ. AZ bis BG.
[24] Agreement on the use and transfer of Passenger Name Records – Ratsentscheidung 2012/472/EU v. 26. 4. 12
[25] Agreement on the processing and transfer of Financial Messaging Data from the EU to the US for the purposes of the Terrorist Finance Tracking Program, - Ratsentscheidung v. 13. 7. 10
[26] Society for Worldwide Interbank Financial Telecommunication. v. 1. 8. 2010
[27] vgl. Bericht der Kommission „Rebuilding trust in EU-US data flows, (COM 2013, 846); Beschluss EU-Parlam. v. 14. 3. 2014 (oben Anm.1) Empfehlungen 53 ff; sowie 24. Tätigkeitsbericht BfDI zu TxtZ. 2.5.1 ff..
[28] vgl. dazu wegen aller Einzelheiten die Mitteilung der Kommission an das Europ.Parlament u. d. Rat über die Funktionsweise der Safe-Harbour Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen v. 27. 11. 13 (Aktz. COM(2013) 847 final; vgl. auch Beschluss Europ.Parl. v. 14. 3. 2014(Anm. 1) TxtZ. BP bis BV.

traulicher Daten. Dabei muss man jedoch bedenken, dass nach der sog. Safe-Harbour-Entscheidung[29] die Datenschutzregeln soweit begrenzt werden können, „als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss." Inzwischen „sind alle Unternehmen, die am Programm PRISM beteiligt sind und den US-Behörden den Zugriff auf in den USA gespeicherte und verarbeitete Daten gestatten, der Safe-Harbour-Regelung beigetreten. Safe Harbour ist auf diese Weise zu einem Informationskanal geworden, über den die US-Nachrichtendienstes auf personenbezogene Daten zurückgreifen können, die ursprünglich in der EU verarbeitet worden sind."[30]

Angesichts der Tatsache, dass die großen Internet-Unternehmen mehrere hundert Millionen Kunden in Europa haben und früher unvorstellbar große Datenmengen zur Verarbeitung in die USA übermitteln, stellt die Kommission die Wirkung der Safe-Harbour-Regelung nun selbst zur Diskussion: "Ernsthaft in Frage zu stellen ist auch, ob die Datenschutzrechte europäischer Bürger, deren Daten in die USA übermittelt werden, angesichts des umfassenden Zugriffs der Nachrichtendienstes auf Daten, die von Safe-Harbour-Unternehmen in die USA übermittelt werden, kontinuierlich geschützt sind."[31]

Die Kommission bemängelt zutreffend den Rechtsschutz, die Transparenz und fordert eine Verpflichtung der Safe-Harbour-Unternehmen, offenzulegen, ob und in welchem Umfang sie personenbezogene Daten an US-Behörden weitergeben.

In der Praxis ist das Cloud Computing in der irrigen Annahme garantierter Vertraulichkeit nach der Safe-Harbour-Zertifizierung geradezu eine besondere Eingriffsquelle der NSA geworden.

g. Schließlich müssen hier die Informationen erwähnt werden, die erst kürzlich über den Stand der Verhandlungen über ein EU – US Datenschutz Rahmenabkommen über den Datenaustausch im justitiellen und polizeilichen Bereich bekannt geworden sind.[32] , die seit 4 Jahren zwischen der EU Kommissarin Vivian Reding und dem US Justizminister Holden nichtöffentlich geführt wurden. Nach dem jetzigen Verhandlungsstand sind alle wesentlichen Streitpunkte offen geblieben. Für Nicht-US-Bürger ist unverändert keinerlei gerichtliche Rechtschutzmöglichkeit vorgesehen und es soll den Vertragspartnern unbenommen bleiben, Datenermittlungen und Verarbeitungen der Geheimdienste und aus Gründen der nationalen Sicherheit von den Regeln des Abkommens auszuklammern. Dass das kein Fortschritt und völlig unannehmbar ist, braucht wohl nicht weiter erörtert zu werden.

f. Insgesamt muss man aus dieser Rechtslage die Folgerung ziehen, dass die Vereinigten Staaten nicht ernsthaft bereit sind, Abstriche von ihrer informationellen Vorherrschaft zu vereinbaren. Es soll dabei bleiben, dass alle Daten dem potentiellen Zugriff der NSA unterliegen, die entweder in den USA gespeichert werden oder die in

---

[29] Entscheidung der EU Kommission v. 26. 7. 2000 - Aktz. 2000/520/EG –Anh. 1.
[30] Bericht der Kommission a.a.O. S. 19
[31] Bericht der Kommission a.a.O. S. 21
[32] vgl. https:Netzpolitik.ORG/2014/internes-dokument-der-EU-Kommission-datenschutz-abkommen v. 16. 4. 2014

Europa Gesellschaften anvertraut werden, die mit US-amerikanischen Providern gesellschaftsrechtlich oder kapitalmässig verbunden sind.

Das Europäische Parlament kommt zu dem Ergebnis, „dass jüngste Enthüllungen durch Informanten und Journalisten in der Presse gemeinsam mit den im Rahmen dieser Untersuchung abgegebenen Sachverständigengutachten, Zugeständnissen von staatlichen Stellen und der Tatsache, dass auf diese Anschuldigungen nicht genügend reagiert wurde, einen zwingenden Beweis für die Existenz weit verzweigter, komplexer und hochmoderner Systeme darstellen, die von den Geheimdiensten der USA und einiger Mitgliedstaaten entwickelt wurden, um die Kommunikationsdaten, darunter Inhalts-, Standort- und Verbindungsdaten aller Bürger weltweit in bisher unbekanntem Ausmaß, wahllos und ohne Vorliegen eines Verdachts zu sammeln, zu speichern und zu analysieren."[33]

Es empfiehlt ausdrücklich, sowohl das Safe-Harbour-Abkommen wie die TFTP und PNR –Abkommen unverzüglich auszusetzen.[34]

7. Nach all dem können wir nun die Frage beantworten, was man von der Kammer und der Bundesregierung in dieser Sache verlangen kann und verlangen muss.

a. Von der Bundesrechtsanwaltskammer muss man zunächst verlangen, dass sie ihre Mitglieder ausdrücklich über die Sach- und Rechtslage ohne jede Beschönigung informiert.
Natürlich könnte man denken, dass gerade international tätige Praxen wissen oder jedenfalls leicht feststellen können, wie die Sach-und Rechtslage ist. Es ist aber ein Unterschied, ob man einen Sachverhalt selbst ermitteln könnte, oder ob man es tatsächlich tut und erkennt, dass es hier nicht nur um das Handy der Bundeskanzlerin oder das Abhören von Einrichtungen des Bundestages oder der Ministerien geht, sondern um die eigene berufliche oder persönliche Kommunikation. Und es geht um die elementare anwaltliche Berufspflicht, das Berufsgeheimnis der ihm von seinen Mandanten anvertrauten Informationen zu wahren.

Zu dieser Aufklärung gehört auch die Veröffentlichung einer „lesbaren" Fassung des Beschlusses des Europäischen Parlamentes v. 12. März 2014. „Lesbar" heißt hier ohne die üblichen Verweisungen auf zahllose andere Dokumente und Erwägungen und eine Beschränkung auf das Wesentliche.

Diese Information ist um so wichtiger, als der Bundestag die Anwaltschaft zwingt, in relativ kurzer Zeit ohne Wahlmöglichkeit zur elektronischen Kommunikation überzugehen und die BRAK alle Vorbereitungen trifft, jeden Anwalt gem. § 31 a BRAO mit einem elektronischen Briefkasten auszurüsten.[35] Jeder anwaltliche Nutzer muss wissen, dass auch bei innerdeutschen Kommunikationen zur Zeit keine Sicherheit dafür besteht, dass seine Informationen tatsächlich vertraulich bleiben.

---

[33] vgl. EP Beschluss v. 12. 3. 2014, Ergebnisse Zif .1.
[34] vgl. EP—Beschluss v. 12. 3. 2014 Empfehlungen 41 und 54
[35] vgl. Ges. z. Förderung d. elektronischen Rechtsverkehrs mit den Gerichten v. 16. 10. 13 (BGBl. I 3786 ff)

b. Der zweite Wunsch an die BRAK ist es, in den Gremien der Kammer und mit der Bundesregierung eingehend zu erörtern, wie der zukünftig zwingend vorgeschriebene elektronische Datenverkehr vor den zur Zeit offenkundig möglichen unberechtigten Zugriffen Dritter zuverlässig geschützt werden kann und bis dahin die Einführung einer anwaltlichen Pflicht zur Nutzung der elektronischen Kommunikation auszusetzen.

c. Der dritte Wunsch an die Kammer ist es, dass sie ggfls. gemeinsam mit anderen Institutionen der freien Berufe oder der gewerblichen Wirtschaft die Bundesregierung dringend auffordert, ihre bisherige beschwichtigende Haltung aufzugeben und die Folgerung daraus zu ziehen, dass es zu keinem völkerrechtlich verbindlichen, mit ausreichenden Sanktionen versehenen, bilateralen Vertrag zwischen der Bundesrepublik und den USA und Großbritannien kommen wird. Die Bundesregierung muss sich auch damit auseinandersetzen, dass ein solches Sonderabkommen als ein Bruch der europäischen Solidarität gesehen und gewertet werden würde, die bei verständiger Würdigung des Sachverhaltes unverzichtbar ist, um gegenüber den Vereinigten Staaten und Großbritannien mit der Forderung Erfolg zu haben, die Grundlagen unserer gemeinsamen Verfassungstradition zu respektieren.

Darum muss sich die Bundesregierung energisch dafür einsetzen, dass

aa. das bisherige Verhandlungsergebnis über ein EU–US Datenschutz-Rahmenabkommen über den Austausch justitieller und polizeilicher Daten öffentlich gemacht und die Verhandlungen nur unter Beteiligung des Europäischen Parlamentes fortgeführt werden,

bb. die Europäische Datenschutz-Grundverordnung noch im Jahr 2014 in Kraft treten kann, zumindest aber der Teil, der alle in der EU erhobenen personenbezogenen Daten dem Schutz der Grundverordnung unterstellt und die in der EU tätigen Unternehmen verpflichtet, ihnen anvertraute oder zugängliche Daten in dritte Staaten nur bei angemessenem Rechtsschutz der Betroffenen auszuleiten und der Kommission anzuzeigen. Dabei muss die Bundesregierung sicherstellen, dass die bisher in Art. 44 der Datenschutz-Grundverordnung vorgesehenen Ausnahmen so massiv eingeschränkt werden, wie es den bisherigen negativen Erfahrungen mit der Safe-Harbour-Regelung entspricht. [36]
Es muss den Anbietern auch möglich sein, verbindlich zuzusichern, dass die Daten eines Kunden nur auf Servern gespeichert und verarbeitet werden, die im Gebiet der Union stationiert sind.

cc. der Rahmen für Bußgelder bei einem Verstoß gegen diese Verpflichtung zumindest auf bis zu 5 % des Umsatzes festgesetzt werden kann, den die Unternehmensgruppe im letzten Jahr in der EU erzielt hatte

---

[36] Bisher haben die Bundesregierung und das EU-Parlament gefordert, dass der Zugriff auf Daten, die dem europ. Datenschutzrecht unterliegen, von der Genehmigung der jeweils zuständigen Datenschutzbehörde des Mitgliedsstaates abhängig gemacht wird.vgl. BFDI-Bericht, oben Anm. 3

dd. Großbritannien hinsichtlich des sog. Tempora-Programms seine Verpflichtung aus der EMRK bzw. den EU-Verträgen erfüllt.

ee. das Safe-Harbour-Abkommen bis zum Ende des Jahres 2014 mit dem Ziel neu verhandelt wird, dass die Kontrollen der zertifizierten Unternehmen konsequent erfolgen und dass die Daten, die unter Berufung auf das Abkommen in den USA oder in zertifizierten Unternehmen gespeichert werden, wie persönliche Daten von US-Staatsangehörigen behandelt werden, also unter dem Schutz des 4. Amendments der Verfassung stehen.

ff. die Abkommen über Passagierdaten und Bankbewegungen in gleicher Weise bis Ende 2014 neu verhandelt werden.

d. Die Bundesregierung sollte formell erklären, dass die genannten Vereinbarungen zunächst ausgesetzt und schließlich gekündigt werden müssen, wenn die geforderten Verhandlungsergebnisse nicht erzielt werden. Zu dem Freihandelsabkommen TTIP sollte die Bundesregierung entsprechend dem Beschluss des EU –Parlamentes ihre Zustimmung davon abhängig machen, dass die Massenüberwachung aufhört und die Rechte der Bürger nach der EU -GRCh respektiert und die Privatsphäre der Bürger geschützt werden.

In diesen Fragen ist Klartext nicht nur wünschenswert, sondern erforderlich. Es ist ein gefälliges Wort, wenn von Freundschaften zwischen Staaten gesprochen wird, ohne zu sagen, was sie in der Wirklichkeit konkret bedeutet. Es kommt darauf an, ob und welche gemeinsamen Interessen man hat, die von beiden Seiten als wichtig betrachtet und gemeinsam verfolgt werden. Dauerhafte gute Beziehungen erfordern und ertragen es, dass diese Interessen und ihre Bedeutung klar definiert und ausgesprochen werden.

e. Die Bundesregierung sollte sich schließlich dafür einsetzen, dass in der EU eine eigene Speicherkapazität eingerichtet wird, die ausschließlich den Regeln des Europäischen Datenschutzes untersteht.

8. Unabhängig von diesen Vorschlägen, sollte die BRAK die Gelegenheit nutzen, die Bundesregierung und den Deutschen Bundestag aufzufordern, die gesetzlichen Regelungen über

a. die unter Art. 10 GG fallenden Ermittlungen des BND im Ausland und die Weitergabe dieser Daten an andere Dienste verfassungsrechtlich einwandfrei zu regeln und

b. die Respektierung der anwaltlichen beruflichen Verschwiegenheitspflicht endlich in Ordnung zu bringen.

Es ist nicht länger hinnehmbar, dass zwar in § 160 a StGB die Zeugnisverweigerungsrechte der Strafverteidiger und aller anderen Rechtsanwälte gleichgestellt worden sind, dass aber die bis dahin geltende Unterscheidung sowohl in § 3 b G 10 Gesetz wie in

§ 20 u BKA-Gesetz beibehalten worden ist, obwohl es für diese Unterscheidung keinen sachlichen Grund gibt. Im Gegenteil: wenn man bei polizeilichen präventiven Ermittlungen bestimmte Berufsgeheimnisse von Rechts wegen durchbrechen kann, dann ist es sinnlos, sie bei der Strafverfolgung bewahren zu wollen.

Die Folge dieser Unterlassung ist, dass wir auch in einer ganzen Reihe von Polizeigesetzen der Bundesländer damit zu kämpfen haben, dass das gegenüber unseren Mandanten und dass diese unterschiedliche Behandlung in arbeitsteiligen Sozietäten zu grotesken Problemen führt.

Dieser Handlungsbedarf besteht unabhängig von den Problemen, die uns die NSA und das GCHQ bereiten.

Burkhard Hirsch