Mitarbeiter des US-Geheimdienstes NSA haben sich nach aller Voraussicht nach deutschem Strafrecht strafbar gemacht. Auch wenn im Ergebnis absehbar keine Verurteilung der Täter vor deutschen Gerichten zu erwarten ist, aber schon die Einleitung eines offiziellen Ermittlungsverfahrens der Bundesanwaltschaft wäre ein wichtiges Signal, das auch die Politik unter Druck setzen würde, die rechtswidrigen Zustände nicht weiter kleinzureden. Das seitens der Bundeskanzlerin in Aussicht gestellte „No Spy-Abkommen“ könnte zumindest klare inhaltliche Positionen für einen transatlantischen Rechtsdiskurs über Spionage und Datenschutz schaffen. Jedoch hilft nur ein Abkommen, welches die Rechte der Bürger auf informationelle Selbstbestimmung nach deutschen Datenschutzstandards gewährleistet und nicht durch weitreichende Ausnahmetatbestände unter dem Vorwand der „Terrorbekämpfung“ aufgeweicht wird, wirklich weiter. Zudem wäre ein europäisches Abkommen mit den USA einem bilateralen, deutsch-amerikanischen Abkommen vorzuziehen. Von **Norbert S. Anschütz**.

Das Ausmaß des von US-amerikanischen National Security Agency (NSA) ausgeführten, in die Teilprogramme „PRISM“, „Mainway“, „Marina“ und „Nucleon“ untergliederten Spähprogramms dürfte selbst düsterste Schreckensszenarien eines modernen Überwachungsstaats in den Schatten gestellt haben.

Den Deutschland betreffenden Kern der möglichen Spionageverbrechen bildet der Verdacht, dass monatlich über fünfhundert Millionen Datensätze aus Kommunikationen deutscher Bürger und in Deutschland lebender Ausländer durch die NSA erhoben wurden.

Die zunächst behauptete, von der Bundesregierung propagierte Beschränkung auf Metadaten trifft nach jetzigen Erkenntnissen nicht zu.

Vielmehr hat Glenn Greenwald im englischen GUARDIAN am 31.07.2013 unter Auswertung weiterer Informationen Edward Snowdens das Programm „Xkeyscore“ enthüllt, mit welchem auch Kommunikationsinhalte umfassend ausgewertet werden.[1]

Mittels „Xkeyscore“ können zuvor gespeicherte, unerschöpfliche Datenbestände nach bestimmten Suchparametern durchforstet werden:

- E-Mail-Postfächer
- Inhalte aus Chat-Rooms
- Internet-Suchanfragen einzelner Nutzer

- Oder kurzum: “nearly everything a typical user does on the internet, including the content of emails, websites visited and searches”[2]

Zuletzt stand die Abhörung des Handys der Kanzlerin im Mittelpunkt der Auseinandersetzung, was verstörenderweise[3] hierzulande die Debatte um rechtliche Gegenmaßnahmen erst richtig (wieder-) entfacht hat.

Die demokratische und rechtsstaatliche Herausforderung ergibt sich vor allem aus einer sehr gefährlichen, das demokratisch-rechtsstaatliche „Immunsystem“ der Bürger atomisierenden Ohnmacht: Den möglichen Spionageverbrechen kann mit den Mitteln des Rechtsstaats scheinbar wenig bis gar nichts entgegengesetzt werden. Die Unverbrüchlichkeit unserer Werteordnung wird in Frage gestellt. Auch dem innerdeutschen und –europäischen Rechtsstaatsdiskurs sind die wahrscheinlichen Spionageverbrechen abträglich: Welcher Gegner kann etwa noch etwas gegen die Vorratsdatenspeicherung einwenden, wenn „eh‘ alles gespeichert“ wird in den USA und es Privatheit schon von daher nicht mehr gibt?

Der nachfolgende Aufriss möchte nicht nur die wahrscheinlichen Spionageverbrechen völker- und strafrechtlich bewerten, sondern vor allem mögliche rechtliche Reaktionsmöglichkeiten ausleuchten – und damit allen tief sitzenden Ohnmachtsgefühlen zum Trotz auch etwas Mut machen, dass die rechtsstaatliche Ausgangslage für eine Verbesserung der Rechtssituation jedenfalls nicht trostlos ist.

Haben die US-Geheimdienste mit ihren Ausspähaktionen das Völkerrecht verletzt?

Einen völkerrechtlichen Vertrag zwischen Deutschland und den USA, der Spionage verbietet, gibt es nicht.[4] Allerdings könnte es ein völkergewohnheitsrechtliches Spionageverbot geben. Dies wird jedoch mit Verweis auf die verbreitete, gemeinhin bekannte und tolerierte Praxis der Staaten, einander „auszuhorchen“, weitgehend abgelehnt.[5]

Sollten die Spionageaktivitäten – wie zuletzt vermutet – aus der amerikanischen Botschaft in Berlin entfaltet worden sein, liegt ein Verstoß gegen das Wiener Übereinkommen über diplomatische Beziehungen von 1961 vor.[6]

Haben sich die Mitarbeiter des NSA oder Regierungsmitglieder der USA nach deutschem Strafrecht strafbar gemacht?

Ja, vorausgesetzt natürlich, die Enthüllungen Snowdens stimmen in den wesentlichen Punkten.

Die Mitarbeiter ausländischer Geheimdienste unterliegen nach den allgemeinen Voraussetzungen der Anwendbarkeit des deutschen Strafrechts dem Strafgesetzbuch (StGB). Strafrechtlich verantwortlich wäre primär der Direktor der NSA. Ihm unterstehende Beamte wären aber ebenfalls verantwortlich. Für den Fall, dass die US-amerikanische Regierung die Ausspähaktionen beauftragt haben sollte, wären auch diese Handelnden „Täter“ im Sinne des deutschen Strafrechts.[7]

An der Anwendbarkeit des StGB könnte man zweifeln, weil die möglichen Täter in den USA sitzen.

Was zunächst Staatsschutzdelikte anbetrifft, so erklärt § 5 Nr. 4 StGB das deutsche Strafrecht auf Taten auch dann für anwendbar, wenn diese im Ausland begangen worden sind.

Einschlägig dürften Delikte zum Schutz von “Staatsgeheimnissen” (§§ 93 ff. Strafgesetzbuch StGB)[8] sowie vor allem der Tatbestand des § 99 StGB, die sog. Geheimdienstliche Agententätigkeit, sein. Die Bedeutung des § 99 StGB: Danach wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wer für den Geheimdienst einer fremden Macht eine geheimdienstliche Tätigkeit gegen die Bundesrepublik Deutschland ausübt, die auf die Mitteilung oder Lieferung von Tatsachen, Gegenständen oder Erkenntnissen gerichtet ist. Damit ist nicht nur das mögliche Ausspionieren von Regierungsmitgliedern erfasst; „gegen die Bundesrepublik“ richten sich vielmehr auch Tätigkeiten in Bezug auf wissenschaftliche oder wirtschaftliche Interessen der Bundesrepublik, weshalb auch etwaige Wirtschaftsspionage erfasst wäre.[9] Gegen die Bundesrepublik richtet sich die Geheimdiensttätigkeit sogar, wenn „andere staatliche und nicht staatliche Strukturen, in denen sich die freiheitliche Demokratie mit ihren Grundrechtsgarantien verwirklicht und weiterentwickelt“, betroffen sind.[10] Wenn Millionen Bürger durch die Ausspähaktionen eingeschüchtert werden und ggf. nicht mehr frei kommunizieren, ist genau ein solches Basiselement der demokratischen Grundordnung betroffen. Damit berührt also auch das Ausspähen der Bürger durchaus den Anwendungsbereich der Staatsschutzdelikte!

Was sodann die Delikte zum Schutz des einzelnen Bürgers betrifft, könnten §§ 201 (Verletzung der Vertraulichkeit des Wortes), 202a (Ausspähen von Daten) sowie 202b StGB (Abfangen von Daten) in einem weiten Umfang verwirklicht sein.[11]

Anders als bei Staatsschutzdelikten, ist hier für die Anwendung des deutschen Strafrechts

jedoch Voraussetzung, dass diese Delikte im Inland begangen worden sind, § 3 StGB. Es genügt dafür zwar, dass der „Deliktserfolg“, also die Verletzung des geschützten Rechtsguts, in Deutschland eingetreten ist. Allerdings wird z.B. zu § 201 StGB die rechtliche Meinung vertreten, dass am Ort des Abgehörten noch kein „Erfolg“ eintritt, da sich das „Abhören“ ja allein am Handlungsort des Abhörenden – hier also den USA – verwirklicht.[12] Folgt man dem – was nicht unumstritten ist – handelt es sich um eine Auslandstat gegen Inländer, und eine Anwendung des deutschen Strafrechts käme nur in Betracht, wenn das Abhören auch nach amerikanischem Strafrecht verboten ist, § 7 StGB. Für §§ 202a und 202b gelten wiederum eigene Erwägungen zum „Erfolgsort“: Hier dürfte es darauf ankommen, an welchem Ort die Daten tatsächlich „abgezweigt“ wurden.

Haben sich Mitarbeiter von Telekommunikationsunternehmen nach deutschem Strafrecht strafbar gemacht?

Es besteht die Vermutung, dass amerikanische Netzanbieter, die Anbindung u.a. an den Frankfurter Datenumschlagplatz haben, Daten abgezweigt und entsprechend ihren Pflichten nach dem amerikanischen Gesetz des Foreign Intelligence Surveillance Act an die NSA weitergeleitet haben.[13]

Etwaige Pflichten zur Datenübermittlung nach US-Recht stellen keinen Rechtfertigungsgrund nach deutschem Strafrecht dar. Hier liegt zumindest Beihilfe zu den o.g. Delikten nahe.

Ist eine Anklage gegen Verantwortliche des NSA wahrscheinlich, oder wird sie auf dem Altar „politischer Opportunität“ geopfert?

Vorab zum Verfahrensstand: Die Bundesanwaltschaft hat ein sog. Vorermittlungsverfahren eingeleitet, das darauf abzielt, zu ermitteln, ob ein Anfangsverdacht für Staatsschutzdelikte besteht. Erst wenn das bejaht wird, wird ein förmliches Ermittlungsverfahren eingeleitet, welches z.B. auch die Vernehmung eines Zeugen Edward Snowden ermöglichte. Wie gerade durch den Sprecher bekanntgegeben, sieht die Bundesanwaltschaft die Voraussetzungen für ein Ermittlungsverfahren bisher noch nicht als erfüllt an,[14] was hoffentlich nur ein Hinweis auf die hohen Sorgfaltsstandards der Behörde bei ihren Vorermittlungen ist.[15] Was das Vorgehen gegen Telekommunikationsunternehmen betrifft, liegt u.a. der Staatsanwaltschaft Flensburg eine Anzeige vor.[16]

Grundsätzlich herrscht das sog. Legalitätsprinzip: Bei einem hinreichenden Tatverdacht muss die Staatsanwaltschaft bzw. bei den Staatsschutzdelikten die Bundesanwaltschaft Anklage erheben.

Für Taten mit Auslandberührung enthält § 153 c StPO aber weitreichende, unter rechtsstaatlichen Gesichtspunkten heftiger Kritik ausgesetzte Ausnahmen von der Verfolgungspflicht, die man mit dem Begriff „Opportunitätsprinzip“ bezeichnet.

Nach § 153 c Abs. 1 Nr. 1 StPO kann die Staatsanwaltschaft von der Verfolgung von Straftaten absehen, die außerhalb des räumlichen Geltungsbereichs des StGB begangen sind. Eine tatbestandliche Einschränkung dieses weiten Ermessens der Ermittler besteht hier nicht.[17]

Nach § 153 c Abs. 3 StPO, der sog. Distanztaten[18] betrifft, kann die Staatsanwaltschaft auch von der Verfolgung von Straftaten absehen, die im räumlichen Geltungsbereich des StGB durch eine außerhalb dieses Bereichs ausgeübte Tätigkeit begangen sind, wenn die Durchführung des Verfahrens die Gefahr eines schweren Nachteils für die Bundesrepublik Deutschland herbeiführen würde oder wenn der Verfolgung sonstige überwiegende öffentliche Interessen entgegenstehen.

Wann genau ist ein solcher schwerer Nachteil für Deutschland zu befürchten? Die juristischen Kommentare nennen hier beispielhaft Gefahren für die äußere Sicherheit oder für den inneren Frieden.[19] Auch das wirtschaftliche Wohl betreffende Nachteile sollen erfasst sein.[20] Die Einschätzungen für den NSA-Skandal gehen dabei auseinander: Während teilweise angenommen wird, dass „[e]ine bloße Abkühlung der Beziehungen zu den USA, die ohnehin zu erwarten ist“ keinen Nachteil in diesem Sinne begründet, so dass das Interesse an der Strafverfolgung überwiegt, [21] gehen andere von der Anwendbarkeit des § 153 c StPO aus. Auch Gegner einer Anwendung des § 153 c StPO USA räumen ein, dass öffentliche Interessen an der Nichtverfolgung jedenfalls dann überwiegen dürften, wenn die USA androhen sollten, Deutschland im Falle einer Anklage nicht mehr an geheimdienstlichen Erkenntnissen teilhaben zu lassen.

Unter diesen Voraussetzungen ist eine Anklage nicht besonders wahrscheinlich.

Wären ein Ermittlungsverfahren und eine Anklage gegen NSA-Mitarbeiter überhaupt erfolgversprechend?

Selbst wenn die Staatsanwaltschaften bzw. die Bundesanwaltschaft die Strafverfolgung nicht aus Opportunitätsgründen nach § 153 c StPO einstellen, ist der Erfolg der Ermittlungen und einer Anklage nicht sicher.

Es müsste ja feststehen, welche Personen konkret gehandelt haben.

Des Weiteren bedürfte es einer hinreichenden Beweisführung. Medienberichte genügten dafür nicht. Hier müssten etwa die offiziellen Unterlagen, die Herr Snowden im Besitz hat, erlangt werden, um sie als Beweismittel in den Prozess einzuführen.[22]

Für Ermittlungen deutscher Strafverfolgungsbehörden im Ausland ist mit einer Kooperation der US-Behörden kaum zu rechnen.[23]

Gelänge es trotz alledem – z.B. unter Mithilfe Snowdens – hinreichende Beweismittel zu erlangen, dürfte der Strafanspruch an der mangelnden Bereitschaft der USA zur Auslieferung seiner Staatsbürger scheitern.

Dennoch wird ein Ermittlungsverfahren teilweise als wichtiges Signal gesehen: „Mit der Einleitung eines Ermittlungsverfahrens würde der Generalbundesanwalt zudem ein wichtiges Signal setzen. Er würde zeigen, dass der im Raum stehende Vorwurf aus deutscher Sicht nicht nur inakzeptabel ist, sondern – sollte er zutreffen – einen schweren Straftatbestand erfüllt und von unserer Rechtsordnung zu Recht missbilligt wird.“[24]

Was ist das „Safe Harbor-Abkommen“, und sollte es ausgesetzt werden?

Grundsätzlich lässt die EU-Datenschutzrichtlinie (Richtlinie 95/46/EG)[25] einen Transfer personenbezogener Daten nur in sichere Drittstaaten zu, die über vergleichbar hohe datenschutzrechtliche Standards verfügen. Dazu zählen die USA nicht. Um dennoch den Transfer von personenbezogenen Daten europäischer Bürger an US-Unternehmen zu ermöglichen, wurde „Safe Harbor“[26] mit dem US-Handelsministerium ausgehandelt und vereinbart. Rechtlich bezeichnet es einen Rechtsakt – einen sog. Beschluss der EU-Kommission. Das Abkommen sieht die Schaffung eines „sicheren Hafens“ für die Daten der EU-Bürger vor, indem Empfänger-Unternehmen in den USA gegenüber der zuständigen US-Behörde erklären müssen, bestimmte Datenschutzgrundsätze zu beachten.[27]

Nach der Einschätzung des Berliner Datenschutzbeauftragten Alexander Dix sind in der Praxis von herausgehobener Relevanz Daten von “Cloud-Dienstleistern” wie Google, Microsoft oder Dropbox: Diese bieten ihre Datenkapazitäten sowohl Unternehmen als auch behördlichen Stellen in Europa an.[28] In den USA unterliegen diese bei den Cloud-Dienstanbietern „gepoolten“ Daten dann dem Zugriff der US-Geheimdienstbehörden.

Mit einer gewissen Berechtigung wird angenommen, dass die Snowden-Aufdeckungen klar zeigten, dass die Voraussetzung für einen „sicheren Datenhafen“, nämlich ein angemessenes Datenschutzniveau in Bezug auf die Empfänger-Unternehmen in den USA, mit nicht mehr besteht. [29]

Die Datenschutzbeauftragten haben bereits Gegenmaßnahmen ihrer Behörden erwogen.[30] Die EU-Kommission sollte aber erwägen, ob nicht überhaupt die Grundlage für diesen Rechtsakt entfallen ist und man „Safe Harbor" daher „aufkündigt".

Der Ausstieg dürfte nicht zuletzt ein Drohmittel von einigem Gewicht sein, das Deutschland bzw. die EU-Kommission bei Verhandlungen mit den USA über ein „No Spy-Abkommen" einsetzen könnten. Immerhin ist die Bedeutung für die US-amerikanische Wirtschaft erheblich: Im Oktober 2010 verzeichnete die entsprechende Liste 3000 US-amerikanische Wirtschaftsunternehmen, die ihren Beitritt erklärt hatten.[31] Darunter befanden sich Größen wie IBM, Microsoft, Amazon, Google, und Facebook.[32]

Was bringt die geplante EU-Datenschutzverordnung?

Ein direkter Fortschritt ist von einer EU-Datenschutzverordnung entgegen anderslautenden Bekundungen vieler Politiker nicht zu erwarten, da diese Verordnung die Frage, welche Überwachungsmaßnahmen im zwischenstaatlichen Verhältnis erlaubt sind, überhaupt nicht regelt.[33]

Mittelbar ist für den hier interessierenden Kontext jedoch wiederum die Frage der Grenzen für die Datenübermittlung durch Unternehmen in Drittstaaten – namentlich die USA – von Belang: Je enger diese Grenzen sind, desto weniger dürfen Konzerne wie etwa Google US-Geheimdienstbehörden Daten zur Verfügung stellen.

Die jüngste Beschlusslage auf Ausschussebene der EU ergibt, dass die sog. Anti-FISA-Klausel wieder Bestandteil des Entwurfs dieser Verordnung wird, nachdem sie zwischenzeitlich aufgrund intensiver Lobbyarbeit der US-Konzerne gestrichen[34] worden war. Im Bericht von *Jan Philipp Albrecht* (MdEP, Grüne) vom 22.10.2013 heißt es dazu: „Datenweitergabe an Drittstaaten: Google und Co. sollen Daten nur auf der Grundlage europäischen Rechts oder darauf beruhender Rechtshilfeabkommen an Behörden in Drittstaaten weitergeben dürfen, sprich: Ohne konkrete Abkommen keine Weitergabe von Daten durch Telekommunikations- und Internetunternehmen."[35] Der entsprechende Artikel 43a ist im jüngsten Entwurf der Verordnung tatsächlich auch wieder enthalten.[36]

Dieses „Verbot unter Erlaubnisvorbehalt" ist wiederum im Zusammenhang mit neuen EU-Sanktionsinstrumenten zu sehen, die gegen Unternehmen zur Anwendung kommen können, die gegen die Verordnung verstoßen. Dazu berichtet Albrecht zusammenfassend: „Verstöße sind keine Kavaliersdelikte und Sanktionen sollen wehtun. Deshalb sollen Unternehmen bis zu fünf Prozent ihres Jahresumsatzes zahlen müssen, wenn sie gegen das neue Gesetz verstoßen. Dies kann bei großen Konzernen bis in Milliardenhöhe gehen und wird

verhindern, dass Unternehmen Datenschutzverletzungen einfach einkalkulieren.“[37]

Der Einschätzung von Thomas Stadler (Internet-Law), der unter Verweis auf den Zugriff der NSA direkt auf Netzknotenpunkte meint, die NSA sei ja gar nicht auf die Datenlieferung der Unternehmen angewiesen,[38] mag für sich genommen zutreffen; doch kann die wesentliche Erschwerung zumindest eines Zugriffsweges auf Datenbestände durchaus als Fortschritt gesehen werden.

Was genau beinhaltet das geplante „No Spy-Abkommen“, und wo liegen die Fallstricke?

Das „No Spy-Abkommen“ ist in aller Munde und soll nach einem Bericht der Frankfurter Allgemeine Sonntagszeitung (FAS) Anfang 2014 ausgehandelt werden.[39]

Seine Bedeutung für die Wiederherstellung rechtsstaatlicher Souveränität und Integrität hängt ganz von drei Faktoren ab:

- Welchen genauen Inhalt wird das Abkommen haben?
- Ist es seiner Rechtsnatur nach verbindlich?
- Welche Sanktionen greifen im Falle eines Verstoßes?

Zum möglichen Inhalt könnte ein Beschluss des (alten) Bundeskabinetts zu einem „Maßnahmenkatalog zur IT-Sicherheit“ aufschlussreich sein. Nach der sich auf diesen Beschluss beziehenden Aussage des amtierenden Innenministers Hans-Peter Friedrich soll das geplante Abkommen vier Punkte umfassen: „Keine Verletzung der jeweiligen nationalen Interessen, keine gegenseitige Spionage, keine wirtschaftsbezogene Ausspähung, keine Verletzung des jeweiligen nationalen Rechts.“

Sollten der dritte und vierte Punkt tatsächlich das sein, was Deutschland in den Verhandlungen mit den USA einfordert, käme das einer kleinen Sensation gleich, [40] würde es doch die bisher seitens der USA geübte Spionage-Praxis weitgehend in Frage stellen. Die Bindung an das deutsche Recht bedeutete insbesondere, dass die NSA künftig sämtliche zum Schutz der Privatheit deutscher Bürger bestehenden Straftatbestände strikt beachten müsste. Wirtschaftsspionage wäre genauso ausgeschlossen, wie das Ausspähen von kritischen Gruppen etwa aus dem Lager der Globalisierungsgegner. Kaum vorstellbar ist allerdings, dass sich die USA nicht Ausnahmen insbesondere unter dem Vorwand der

„Terrorismusabwehr“ ausbedingen werden. Und hier beginnen dann im Detail wieder die Probleme: Dürfen also doch wieder Verkehrsdaten und sogar Kommunikationsinhalte auf Vorrat gespeichert werden, um sie im konkreten Verdachtsfall auswerten zu können? Der Grundsatz der „Datensparsamkeit“, der bekanntlich den einzig wirksamen Datenschutz gewährleistet, würde so wiederum verletzt. Und wer kann garantieren, dass die so weiterhin gespeicherten Daten nicht doch zu anderen Zwecken verwendet werden?

Ebenso offen wie der Inhalt, ist die beabsichtigte Rechtsnatur des Abkommens. Geht es nur darum, „Kritik aus Deutschland den Wind aus den Segeln zu nehmen“[41]? Der Völkerrechtler Stefan Talmon von der Universität Bonn hat kürzlich auf die unverbindliche Rechtsnatur bisheriger „No Spy-Abkommen“ hingewiesen: „Alle bestehenden sogenannten No-Spy-Abkommen sind in Wirklichkeit bloße Memoranda of Understanding“. [42] Das bedeutet, dass es sich um politische Zweckerklärungen handelt, aber nicht um völkerrechtlich verbindliche Verträge.

Aber auch für den Fall eines völkerrechtlichen Vertrags dürfte die praktische Bedeutung nicht überschätzt werden: Es ist anzunehmen, dass sich die USA wie bisher, auch für dieses Abkommen nicht der Rechtsprechung des Internationalen Strafgerichtshof (IGH) in Den Haag unterwerfen, so dass es an effektiven Sanktionen mangeln wird.[43]

Darüber hinaus lässt sich ein bilateraler „Schnellschuss“ auch aus europäischer Perspektive mit beachtlichen Gründen kritisieren. So äußert der Europaabgeordnete Albrecht (Grüne) eine berechtigte Sorge: „Die Frage ist, ob die Europäer sich wieder gegeneinander ausspielen lassen, wie es schon so oft der Fall war“.[44] Die europäische Perspektive sollte man nicht unterschätzen: Könnte ein „No Spy-Abkommen“ zwischen den USA und der EU ausgehandelt werden, stünde den USA im Falle neuerlicher Verstöße die gesamte europäische Rechtsgemeinschaft gegenüber! Dies würde die abschreckende Wirkung durchaus erhöhen.

In den kommenden Wochen und Monaten kommt es für die kritische Gegenöffentlichkeit darauf an, die Entwicklungen zu diesem Abkommen sehr dezidiert zu begleiten. Selbst wenn – wie zu erwarten – die Perspektive einer IGH-Jurisdiktion fehlt: Die Wirkung, dass es (möglichst) in einem völkerrechtlichen Vertrag „schwarz auf weiß“ steht, was US-Geheimdiensten nicht mehr erlaubt ist, ist bedeutsam für den nationalen wie internationalen (transatlantischen) rechtsstaatlichen Diskurs. „Kein demokratischer Rechtsstaat lässt sich gerne vorhalten, völkerrechtswidrig zu handeln“, wird der Kölner Völkerrechtler *Nikolaos Gazeas zitiert*,[45] und ihm ist in dieser Einschätzung voll zuzustimmen.

Resümee: Mitarbeiter des US-Geheimdienstes NSA haben sich nach aller Voraussicht nach deutschem Strafrecht strafbar gemacht. Auch wenn im Ergebnis absehbar keine Verurteilung der Täter vor deutschen Gerichten zu erwarten ist: Schon die Einleitung eines offiziellen Ermittlungsverfahrens der Bundesanwaltschaft wäre ein wichtiges Signal, das auch die Politik unter Druck setzen würde, die rechtswidrigen Zustände nicht weiter kleinzureden.

Das seitens der Bundeskanzlerin in Aussicht gestellte „No Spy-Abkommen“ könnte zumindest klare inhaltliche Positionen für einen transatlantischen Rechtsdiskurs über Spionage und Datenschutz schaffen. Jedoch hilft nur ein Abkommen, welches die Rechte der Bürger auf informationelle Selbstbestimmung nach deutschen Datenschutzstandards gewährleistet und nicht durch weitreichende Ausnahmetatbestände unter dem Vorwand der „Terrorbekämpfung“ aufgeweicht wird, wirklich weiter. Zudem wäre ein europäisches Abkommen mit den USA einem bilateralen, deutsch-amerikanischen Abkommen vorzuziehen.

[«1] Greenwald

[«2] Zitiert nach Greenwald

[«3] Albrecht Müller mit der Frage: „Sind wir schon so verblödet, dass wir uns erst dann aufregen, wenn Frau Merkel von den US-Diensten abgehört wird?“

[«4] Talmon

[«5] Talmon

[«6] Talmon

[«7] Interview mit Gazeas [PDF – 107 KB]

[«8] Einschätzung von Safferling

[«9] Lampe/Hegmann, in: Münchener Kommentar zum StGB, 2. Auflage 2012, § 99 Rn. 15.

[«10] Lampe/Hegmann, in: Münchener Kommentar zum StGB, 2. Auflage 2012, § 99 Rn. 15.

[«11] Vgl. Interview mit Safferling

[«12] Böse, in: Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 4. Auflage 2013, § 9 Rn. 10.

[«13] Vgl. zu dem Verdacht gegen das Unternehmen „Level 3“: „Im Verdacht stehen große Netzwerkbetreiber wie der US-Konzern Level 3, die auch in Deutschland Infrastruktur betreiben und viel Datenverkehr an Internetknoten abwickeln. Geheimdienste könnten diese Firmen zur Kooperation zwingen, Datenverkehr aus deren Netzen kopieren und in Echtzeit zur Analyse in eigene Systeme leiten. In den Vereinigten Staaten müssen Telekom-Unternehmen solche Abhörschnittstellen installieren.“

[«14] dradio

[«15] Kritisch zum Vorgehen der Bundesanwaltschaft Gauweiler, vgl. hier

[«16] Dazu das Interview mit dem Anzeigeerstatter, Rechtsanwalt Udo Vetter

[«17] Schoreit, in: Karlsruher Kommentar zur StPO, 6. Auflage 2008, § 153c Rn. 1.

[«18] Dabei handelt es sich um Inlandstaten iSv §§ 3, 9 StGB, so dass hierauf § 153 c Abs. 1 Nr. 1 StPO nicht anwendbar ist.

[«19] Schoreit, in: Karlsruher Kommentar zur StPO, 6. Auflage 2008, § 153c Rn. 14.

[«20] Pfeiffer, Strafprozeßordnung, 5. Auflage 2005, § 153 c Rn. 5.

[«21] Interview mit Gazeas [PDF – 107 KB]

[«22] Interview mit *Safferling*

[«23] Interview mit *Safferling*

[«24] Interview mit Gazeas [PDF – 107 KB]

[«25] Amtsblatt der Europäischen Gemeinschaften [PDF – 512 KB]

[«26] Amtsblatt der Europäischen Gemeinschaften [PDF – 512 KB]

[«27] Vgl. Klug, RDV 2000, 212; Heil, DuD 2000, 444.

[«28] Dix – Datenschutz ist keine Privatsache

[«29] Dix – Datenschutz ist keine Privatsache

[«30] Vgl. etwa die Aussage von Dix: „Für diesen Fall haben die europäischen Aufsichtsbehörden nach den Entscheidungen der EU-Kommission das Recht und nach meiner Auffassung auch die Pflicht, keine weiteren Genehmigungen für den Datenexport in die USA zu erteilen und zu prüfen, inwieweit genehmigungsfreie Übermittlungen ausgesetzt werden müssen. Außerdem hat die Europäische Kommission selbst angekündigt, bis Ende des Jahres entscheiden zu wollen, ob das Safe-Harbor-Abkommen gekündigt werden soll."

[«31] *Gola/Schomerus*, Bundesdatenschutzgesetz, 11. Auflage 2012, § 4 b Rn. 15.

[«32] Safe Harbor

[«33] Kritisch zum fehlleitenden Diskurs daher zu Recht Stadler

[«34] Dazu insbesondere

[«35] The Greens – Datenschutzgrundverordnung in 10 Punkten [PDF – 33.4 KB]

[«36] Der Entwurf findet sich hier [PDF – 562 KB]

[«37] The Greens – Datenschutzgrundverordnung in 10 Punkten [PDF – 33.4 KB]

[«38] Internet Law – Der Datenschutz bietet keine Handhabe gegen die Überwachungspraxis der Geheimdienste

[«39] FAZ – Berlin und Washington einig – „No-Spy-Abkommen" kommt bald

[«40] Ähnlich die Einschätzung von Müller: „Wenn mit diesem – bisher nur angekündigten – Vertrag verboten wird, dass Nachrichtendienste Regierungsstellen, Botschaften und Behörden des anderen Staates ausspähen, wenn die Sammlung von Daten untersagt werden soll, die sich gegen die Interessen des anderen Landes richtet, dann wäre das alles andere als eine Selbstverständlichkeit. Das gilt ebenso für den beabsichtigten Verzicht auf Wirtschaftsspionage sowie auf das Ausforschen geistigen Eigentums."

[«41] Müller

[«42] Zitiert nach Bubrowski/Bannas

[«43] FAZ – NSA-Affäre – Wo das Recht endet

[«44] FAZ – Berlin und Washington einig – „No-Spy-Abkommen" kommt bald

[«45] Sueddeutsche – Politisch peinlich, faktisch folgenlos