Dieter Deiseroth

NSA-Ausspähungen und der demokratische Verfassungsstaat

Neun Thesen zum rechtspolitischen Handlungsbedarf

Dieter Deiseroth bewertet die NSA-Affäre aus einer völkerrechtlichen Perspektive. Sein Ergebnis: Obwohl das Recht auf informationelle Selbstbestimmung bisher nur sehr unzureichend in den internationalen Menschenrechtsverträgen verankert ist, stellen die Überwachungsaktivitäten der NSA und deren Verbündeter einen klaren Verstoß gegen das Völkerrecht dar, der auch mit den Mitteln des deutschen Strafrechts zu ahnden ist – wenn der (politische) Wille dazu vorhanden wäre.

Deiseroth formuliert in seinem Beitrag neun konkrete Handlungsempfehlungen. Sie reichen von der Offenlegung und Klärung möglicherweise noch bestehender Sonderregelungen mit den ehemaligen Alliierten, einer Stärkung parlamentarischer Kontrollbefugnisse sowie einem ausnahmslosen gerichtlichen Individualrechtsschutz gegen geheimdienstliche Überwachungsmaßnahmen bis zu neu zu schaffenden supranationalen Vereinbarungen zum Datenschutz zwischen der EU und den USA.

Die weltweite intensive Fahndung der US-Behörden nach Edward J. Snowden als einem „hochkriminellen Landesverräter“ mit all ihren Begleiterscheinungen[1] und die dies rechtfertigenden offiziellen Erklärungen von US-Präsident Obama und anderen Amtsträgern können nur so verstanden werden, dass dieser Whistleblower offenkundig empfindliche, für die US-Regierung und ihre Verbündeten peinliche Wahrheiten aufgedeckt hat,[2] darunter die jahrelange Überwachung des Mobiltelefons der deutschen Kanzlerin und von Datensätzen ungezählter Bürgerinnen und Bürger in Deutschland.

Hochrangige US-Vertreter erklären bis heute mantraartig, sie verstünden die ganze Aufregung nicht: Das meiste sei doch ohnehin bekannt; jedenfalls hätten die deutsche Regierung und ihre Nachrichtendienste „es“ wissen müssen; zudem profitierten die Deutschen im „Kampf gegen den Terror“ von den dadurch erzielten nachrichtendienstlichen Aufklärungserfolgen. Alles vollziehe sich auf dem Boden des geltenden Rechts.

Mittel und Wege der Datenbeschaffung

Die NSA und andere Dienste setzen auf eine Vielzahl unterschiedlicher Methoden, um weltweit für ihre Zwecke geeignete Daten zu erheben. Nach den von Snowden enthüllten Dokumenten[3] geschieht dies u.a. direkt bei amerikanischen IT-Unternehmen wie Google, Apple, Facebook, Microsoft, durch in IT-Software oder in Hardware eingebaute „Hintertüren“, durch Anzapfen von Unterwasser-Glasfaserkabeln und von Satellitenfunkverkehr sowie durch unbefugtes Eindringen in Internet-Knotenpunkte. Anfang Oktober 2014 ist ferner bekannt geworden, dass das deutsche Auswärtige Amt in den Jahren 2011 und 2012 über 110 US-Unternehmen gestattet haben soll, in Deutschland „analytische Dienstleistungen“ für die US-Streitkräfte zu erbringen. Dahinter kann sich die nachrichtendienstliche Auswertung von Datennetzen verbergen. Aktuell sollen in Deutschland 44 solcher Verträge mit „Geheimdienstfirmen“ bestehen.

Soweit die NSA und andere US-Dienste sich die Daten in den USA beschaffen, können sie sich dort auf US-Rechtsvorschriften berufen, insbesondere den 2008 novellierten *US-Foreign Intelligence Surveillance Act* (FISA)[4] und den *USA-Patriot-Act* von 2001[5]. Dies betrifft auch den Datenverkehr, der über das Internet von ausländischen Nutzern „durch“ die USA „fließt“ oder der bei - dem US-Recht unterliegenden - IT-Unternehmen anfällt. Denn der Internet-Datenverkehr kennt keine Grenzen. E-Mails und andere digitale Datensätze werden, auch wenn Sender und Empfänger sich etwa in Deutschland befinden, über die Netzverbindungen geleitet, die global dafür offenstehen und ad hoc am kostengünstigsten erscheinen.

Da US-IT-Unternehmen im weltweiten Internet-Verkehr eine dominierende Rolle spielen, gelangen diese Datenströme auf diese Weise in die USA und unterliegen damit dem dortigen Zugriff der US-Dienste. Dies gilt etwa für Daten aus der digitalen Internet-Kommunikation innerhalb Deutschlands jedenfalls so lange, wie die Deutsche Telekom ihre Ankündigung vom Oktober 2013 nicht umgesetzt hat, durch geeignete technische Maßnahmen „den deutschen Internetverkehr innerhalb der Landesgrenzen zu belassen, um die Kunden vor Spionage aus dem Ausland zu schützen“.[6]

Der Zugriff der NSA und kooperierender Dienste auf die Kommunikationsdaten erfolgt ausweislich der Enthüllungen Snowdens und anderer Whistleblower freilich nicht nur in den USA, sondern auch außerhalb des US-Hoheitsgebietes. Dabei kann es sich um staatsfreie Bereiche (z.B. auf „Hoher See“ oder im Weltraum), aber auch um Hoheitsgebiete anderer Staaten handeln.

Diese Datenerhebungen durch die US-Dienste sind Ausübung von Staatsgewalt, welche auf dem Gebiet anderer Staaten grundsätzlich unzulässig ist.[7] Die genannten US-Gesetze können keinen Datenzugriff innerhalb von ausländischen Hoheitsgebieten rechtfertigen. Dafür fehlt dem US-Gesetzgeber die Kompetenz. In einem ausländischen Hoheitsgebiet darf ein Staat nur das tun, was das Recht dieses Staates erlaubt. Es ist völkerrechtlich nicht im Streit,[8] dass ein Staat bei Fehlen einer solchen Erlaubnisnorm Hoheitsgewalt im Staatsgebiet eines ausländischen Staates nicht ausüben darf. Er ist damit für jede hoheitliche Betätigung und damit auch für Eingriffe in Rechte von Bürgern völkerrechtlich auf die Zustimmung des betreffenden Staates angewiesen. Es gibt zwar weder im Völkervertrags- noch im Völkergewohnheitsrecht

ein umfassendes Verbot der Spionage gegen einen fremden Staat. Ebenso gibt es im Völkerrecht aber auch keine positive Erlaubnisnorm für Spionage und nachrichtendienstliche Tätigkeit; dies gilt jedenfalls für Friedenszeiten.[9] Die gleiche Völkerrechtsordnung, die Spionage nicht als völkerrechtliches Delikt der Staaten einordnet, stellt es den Staaten zugleich aber frei, Spionage mit allen erforderlichen Mitteln abzuwehren, auch und insbesondere mit den Mitteln des nationalen Strafrechts.[10]

Es ist völkergewohnheitsrechtlich anerkannt und entspricht der ständigen Staatenpraxis sowie allgemeiner Rechtsüberzeugung aller Rechtskreise, dass Personen, die eine nachrichtendienstliche Tätigkeit (Agententätigkeit) in einem anderen Staat ohne dessen Zustimmung ausüben, dafür vom ausspionierten Staat bestraft werden dürfen und dass nachrichtendienstliche Tätigkeit vom davon betroffenen Staat abgewehrt und verhindert werden darf.

Rechtfertigungen

NSA-Chef Keith Alexander rechtfertigte die globalen anlasslosen Überwachungs-Aktivitäten seines Geheimdienstes wiederholt mit der notwendigen Terrorismus-Abwehr. Seit dem 11.9.2001 seien auf diese Weise mehr als 50 Anschläge in 20 Ländern verhindert worden. Darunter fanden sich nach offizieller Darstellung auch Hinweise, die zur Aufdeckung der Pläne der sogenannten „Sauerland-Gruppe“ in Deutschland geführt haben sollen. Die im Januar 2014 publizierte US-Studie „Do NSA's Bulk Surveillance Programs Stop Terrorists?“[11] der parteiunabhängigen *New America Foundation* stellt diesen Zusammenhang freilich fundamental in Frage. Nach Auswertung von 225 verfolgten Terrorfällen kommt die Stiftung zu dem Schluss, die Sammlung von Daten im Telefon- und Internetverkehr habe „bestenfalls in 1,8 Prozent der Fälle eine nachweisbare Rolle gespielt.“ Tatsächlich seien traditionelle Ermittlungs-Methoden für die Erfolge verantwortlich: „Informanten, Tipps aus örtlichen Nachbarschaften und gezielte Geheimdienst-Operationen waren der Auslöser für die meisten Untersuchungen.“ Nachprüfbare Fakten, die einen gegenteiligen Schluss rechtfertigen könnten, wurden bisher weder von den US-Behörden noch von deutschen Stellen auf den Tisch gelegt.

Selbst wenn es sie gäbe: Eine anlasslose Speicherung der Tele- und Internet-Kommunikationsdaten ist gerade deshalb ein so schwerwiegender Eingriff in fundamentale Menschenrechte, weil sie in unvorhersehbarer Weise tiefe Einblicke in das Privatleben erlaubt, ohne dass der Rückgriff auf die Daten für den Bürger unmittelbar spürbar oder ersichtlich ist. Der Einzelne weiß nicht, was welche staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können. Ohne Kenntnis können die Betroffenen weder eine Unrechtmäßigkeit der behördlichen Datenerhebung und -verwendung noch etwaige Rechte auf Löschung, Berichtigung oder Genugtuung geltend machen. Das ist von größter Brisanz.

Dabei ist in Rechnung zu stellen, dass die in die Verfügungsgewalt von US-Nachrichtendiensten gelangten Daten Grundlage für die weltweite geheime US-Drohnenkriegsführung sind, in deren Rahmen US-Präsident Obama nach geheimdienstlichen

Listen über die Exekution von Verdächtigen ohne jedes gerichtliche Verfahren entscheidet. Die 2013 publizierte Studie „Geheimer Krieg“ von Christian Fuchs und John Goetz hat hierzu umfangreiches Material vorgelegt.

Eine geheime Informationsbeschaffung und Datenverwaltung durch Nachrichtendienste und andere Sicherheitsbehörden ist von deren spezifischen „bias“-Strukturen geprägt: Nachrichtendienste sehen die Welt mit anderen Augen als etwa Wissenschaftler oder Gerichte und unterliegen anderen Anerkennungs- und Rechtfertigungsmustern. Wegen der fehlenden kontinuierlichen kritischen Hinterfragung im öffentlichen Diskurs sind die von ihnen gewonnenen Daten und Erkenntnisse strukturell defizitär und damit besonders fehleranfällig. Innerbehördliche Überprüfungen können dies nach allen Erfahrungen mit dem Wirken von nur partiell kontrollierten Geheimbehörden nicht ersetzen.

Wirksame Kontrollen durch Parlamente und Gerichte erfolgen nur sehr begrenzt. Mitarbeiter der Geheimdienste, die vor Parlamentsgremien oder Gerichten aussagen sollen, erhalten u.a. unter Berufung auf „Quellenschutz“ vielfach nur sehr eingeschränkte Aussagegenehmigungen. Zumeist dürfen sie nicht einmal angeben, von wem sie die Informationen erhalten haben, sondern lediglich mitteilen, dass ihrer Dienststelle glaubwürdige Informationen über ein bestimmtes Thema oder eine bestimmte Person vorlägen.

Die Verlässlichkeit der Quellen und der von diesen tatsächlich oder angeblich gelieferten Daten kann so nicht in einem rechtsstaatlichen Verfahren kritisch überprüft werden. Auf einer solchen Grundlage lassen sich Informationen weder verifizieren noch widerlegen. Zudem sind Gerichte in den USA[12] wie auch in Deutschland[13] vielfach äußerst großzügig bei der Zubilligung von Einschätzungsspielräumen der Exekutive gerade im nachrichtendienstlichen Bereich.

Privatsphäre und Demokratie

Der Schriftsteller Ilya Trojanow erklärte gegenüber der NZZ:

> *„Heute gehen die informationssaugenden Behörden nicht mehr von einem verdächtigen Individuum aus, dessen Verhalten und Kommunikation zu überwachen ist, sondern von einer verdächtigen Gesellschaft, die als Ganze durchleuchtet werden muss, um die Gefährlichen, Auffälligen, Kritischen und Renitenten herauszufischen.“*[14]

Viele Kritiker sehen dies ähnlich. Manche versuchen dies zu bagatellisieren. Zur Rechtfertigung der anlasslosen Überwachungsmaßnahmen hört man häufig: „Wer nichts zu verbergen hat, hat auch nichts zu befürchten.“ Dieser scheinbar plausible, letztlich aber unverschämte Satz ist, leider, Allgemeingut geworden und fördert die Duldungsstarre der Bürger. Man könnte zurückfragen: „Wenn ich nichts zu verbergen habe, warum wollt Ihr das dann wissen?“

Häufig wird behauptet, die Bürgerinnen und Bürger seien im Übrigen letztlich selbst schuld, wenn andere auf ihre persönlichen Daten so leicht Zugriff nehmen könnten. Denn sie seien selbst in erster Linie für deren Schutz verantwortlich. Ein solches Argument ist eher zynisch. Auch wenn viele Bürger etwa in ihren E-Mails und in den sozialen Netzwerken wie Facebook, Twitter etc. recht großzügig ihre eigenen Daten zugänglich machen, ist klar: Grundrechtsschutz ist und bleibt unverzichtbar eine zentrale Aufgabe und Verpflichtung der staatlichen Organe eines demokratischen Verfassungsstaates.

Es geht dabei nicht nur um den Schutz von Privatheit, sondern vor allem um fundamentale Werte und Strukturen eines demokratischen Gemeinwesens. Demokratie ist ohne einen demokratischen Meinungs- und Willensbildungsprozess nicht möglich. Das Demokratiegebot des Grundgesetzes findet sich nicht mit einer „Zuschauerdemokratie“ ab. Es gewährleistet die aktive Teilnahme aller Bürgerinnen und Bürger am politischen Meinungs- und Willensbildungsprozess, der nicht von den Regierenden zu den Regierten, also nicht von „oben nach unten“, sondern gerade umgekehrt von „unten nach oben“ verlaufen muss. Daten-Abstinenz hilft da nicht, im Gegenteil. Demokratie erfordert, dass sich die Bürgerinnen und Bürger im öffentlichen Raum, in den Medien und auch im Netz sichtbar machen, um Gehör zu finden und öffentliche Wirkung zu erzielen. Demokratische Partizipation und Mitbestimmung in prinzipiell allen gesellschaftlichen Angelegenheiten sind nur möglich, wenn sich die Stimmen der engagierten Bürgerinnen und Bürger zu Gehör bringen und Niederschlag in den Kommunikationsbeziehungen finden.

Demokratie verträgt freilich keine für die „Obrigkeit“ „gläsernen“ und „durchsichtigen“ Bürger. Für ein demokratisches Gemeinwesen ist und bleibt von zentraler Bedeutung: Die Bürgerinnen und Bürger dürfen als der demokratische Souverän nicht mit Hilfe von Algorithmen und Datenbanken für die von ihnen zu kontrollierenden Machtinstanzen „von oben nach unten“ berechenbar gemacht werden. Sie müssen für die „Obrigkeiten“ letztlich „undurchschaubar“ sein und bleiben. Nur dann sind sie der „demokratische Souverän“, von dem in einer Demokratie alle Staatsgewalt auszugehen hat.

Rechtspolitischer Handlungsbedarf - Neun begründete Thesen

These 1: Ohne Whistleblower sind wir den Datenangriffen der NSA und anderer Dienste weithin schutzlos ausgeliefert, weil wir nicht einmal davon erfahren.

Whistleblower, die solche schweren Angriffe auf Menschenrechte aufdecken und enthüllen, benötigen Hilfe und Unterstützung.[15] Das erfordert einen wirksamen Whistleblower-Schutz auf allen Ebenen.[16] Notwendige Schutzregelungen müssen u.a. die Aufnahme solcher Whistleblower in ein Zeugenschutzprogramm, einen gesicherten Aufenthaltsstatus, den Schutz vor Auslieferung und Bestrafung, die Sicherung des Existenzminimums und Hilfen bei der gesellschaftlichen Integration gewährleisten.

Bei dieser Schutzaufgabe sind der nationale Gesetzgeber sowie die nationale und die internationale Rechtsprechung gefordert. Außerdem sind internationale Regelungen in völkerrechtlichen Abkommen erforderlich. Die Zivilgesellschaften müssen hier für den notwendigen Druck sorgen.

These 2: Bei Vorliegen eines Anfangsverdachts, also von tatsächlichen Anhaltspunkten für die Möglichkeit eines Verstoßes von Nachrichtendiensten gegen Strafrechtsnormen zum Schutz des Post- und Fernmeldegeheimnisses und persönlicher Daten muss entsprechend dem Legalitätsprinzip unverzüglich von den Strafverfolgungsbehörden ein Ermittlungsverfahren eingeleitet und wirksam betrieben werden. Dies gilt nicht nur dann, wenn es um das Abhören des Mobiltelefons der Bundeskanzlerin geht. Gegen jeden Amtswalter, der sich weigert, wirksame Ermittlungsmaßnahmen einzuleiten und durchzusetzen, muss ein Verfahren wegen Strafvereitelung im Amt durch die örtlich zuständige Staatsanwaltschaft eingeleitet werden.

Durch illegale Ausspäh- und Abhöraktionen kann neben dem Grundrecht auf Schutz des Post- und Fernmeldegeheimnisses (Art. 10 Abs. 1 Grundgesetz - GG) vor allem das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 u. Art. 1 GG), also die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, bedroht und verletzt werden. Aber auch das Grundrecht auf Wahrung der Vertraulichkeit und der Integrität informationstechnischer Systeme (Art. 2 Abs. 1 u. Art. 1 Abs. 1 GG) kann betroffen sein. Gleiches gilt, wenn mit akustischer und optischer Wohnraumüberwachung sowie mit der Messung von elektromagnetischer Abstrahlung, die mit der Nutzung von IT-Systemen verbunden ist, eingegriffen wird; dann kann das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 GG) beeinträchtigt sein.

Die zuständigen deutschen Stellen sind gem. Art. 1 Abs. 3 GG verpflichtet, unzulässige Beeinträchtigungen der Grundrechte mit allen zu Gebote stehenden Mitteln zu verhindern.[17] Dem dient u.a. das Strafrecht. Die Verletzung dieser Rechte ist in Deutschland in weitem Maße unter Strafe gestellt. Dies gilt etwa für die Verletzung der Vertraulichkeit des Wortes (§ 201 StGB), die Verletzung des Briefgeheimnisses (§ 202 StGB), das Ausspähen von Daten (§ 202a StGB), das Abfangen von Daten (§ 202b StGB), das Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB) und die Verletzung des Post- oder Fernmeldegeheimnisses (§ 206 StGB).

Die Rechtswidrigkeit und Strafbarkeit entfallen bei Ausspähaktionen der NSA und anderer Dienste in Deutschland nicht etwa deshalb, weil und soweit sich diese Dienste auf nationale gesetzliche Ermächtigungen des US-Gesetzgebers nach dem US-Patriot Act oder dem FISA-Gesetz oder auf eine Executive-Order des US-Präsidenten stützen können. Nationales US-Recht vermag außerhalb der USA grundsätzlich keine Rechtsbrüche und Straftaten, die in Deutschland oder anderswo begangen werden, zu legitimieren und straffrei zu stellen.

Das deutsche Strafrecht gilt gemäß § 3 StGB zum einen für alle Straftaten, die im Inland, also in Deutschland, begangen werden. Eine Straftat ist an jedem Ort begangen, an dem der Täter gehandelt hat oder an dem der zum Tatbestand gehörende Er-

folg eingetreten ist oder nach der Vorstellung des Täters eintreten sollte (§ 9 StGB). Das deutsche Strafrecht gilt nach § 7 Abs. 1 StGB aber außerdem auch für Taten, die im Ausland gegen einen Deutschen begangen werden, wenn die Tat am Tatort mit Strafe bedroht ist oder der Tatort keiner Strafgewalt unterliegt (z.B. auf Hoher See).

Unabhängig vom Recht des Tatortes gilt das deutsche Strafrecht nach § 5 StGB zudem u.a. für folgende im Ausland begangene Taten, die nach dem StGB strafbar sind: Landesverrat (§ 94 StGB), landesverräterische Ausspähung (§ 96 StGB), landesverräterische Agententätigkeit (§ 98 StGB) und geheimdienstliche Agententätigkeit (§ 99 StGB), eine Strafbestimmung, die etwa für das Ausspähen des Mobiltelefons der Bundeskanzlerin Merkel von besonderer Bedeutung ist.

These 3: Artikel 10 Grundgesetz und das G-10-Gesetz müssen reformiert werden.

(1) Das Ausführungsgesetz zu Art. 10 GG (G10-Gesetz) gewährt den Nachrichtendiensten der Bundesrepublik ausgedehnte Kompetenzen zum nachrichtendienstlichen Ausspähen von personenbezogenen Daten im In- und Ausland. Es gilt für die Verfassungsschutzbehörden des Bundes (BfV) und der Länder (LfV), den Militärischen Abschirmdienst (MAD) sowie den Bundesnachrichtendienst (BND).

Den Geheimdiensten und den Truppen der USA und anderer Entsendestaaten in Deutschland gewährt das G10-Gesetz jedoch keine eigenständigen Überwachungsbefugnisse. Die US-Stellen können sich allerdings nach den bestehenden völkerrechtlichen Vereinbarungen an die zuständigen deutschen Stellen wenden und um die Durchführung nachrichtendienstlicher Eingriffe in das Post- und Fernmeldegeheimnis nach Maßgabe des G10-Gesetzes sowie um Datenübermittlung (§ 7a Abs. 2 G10-Gesetz) durch diese nachsuchen. Gehen solche Gesuche beim BND oder beim BfV ein, müssen diese bei dem zuständigen deutschen Ministerium – auf Bundesebene das Bundesinnenministerium (BMI) – im eigenen Namen die Anordnung der gewünschten Eingriffe in das Post- und Fernmeldegeheimnis beantragen und anschließend „alle erforderlichen Maßnahmen“ veranlassen.

Solche deutschen Überwachungsmaßnahmen können sowohl nach § 3 („Abwehr von drohenden Gefahren“ im Einzelfall) als auch nach § 5 G10-Gesetz („strategische Überwachung“) und nach § 8 G10-Gesetz (z.B. Rettung aus Gefahr für Leib oder Leben im Ausland) vom Bundesinnenministerium angeordnet werden. Zuvor bedarf es jedoch nach dem G10-Gesetz der Zustimmung durch die vom Bundestag gewählte, aus vier Mitgliedern bestehende G10-Kommission, die von Amts wegen oder auf Grund von Beschwerden über die Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen entscheidet (§ 15 Abs. 5 G10-Gesetz). Das betrifft damit auch Maßnahmen, die von den US-Streitkräften beantragt worden sind. Die Kontrollbefugnis der G10-Kommission erstreckt sich auf die Erhebung, Verarbeitung und Nutzung aller nach diesem Gesetz erlangten personenbezogenen Daten durch Nachrichtendienste des Bundes.

Auf Wunsch haben BND und BfV den alliierten Dienststellen die Anwesenheit bei Beschränkungsmaßnahmen zu gestatten. Ferner sind sie verpflichtet, nicht nur die Ergebnisse der Überwachungsmaßnahme, sondern das gesamte angefallene Material den westlichen Diensten zu übergeben.

(2) Angesichts der jüngsten Enthüllungen von Snowden und anderer Whistleblower stellt sich jedoch die Frage, ob neben dem G10-Gesetz (§ 7a Abs. 2) in Deutschland darüber hinaus ferner bisher nicht bekannte Rechtsgrundlagen für eigenständige Überwachungsbefugnisse der Stationierungsstreitkräfte und ihres zivilen Gefolges innerhalb des deutschen Hoheitsgebietes bestehen. Das ist weder im G10-Gesetz noch sonst klar geregelt. Hier besteht Klärungsbedarf.

(3) Handlungsbedarf besteht auch hinsichtlich des Rechtsschutzes gegen nachrichtendienstliche Überwachungen. Seit der Änderung des Art. 10 GG und des Art. 19 Abs. 4 S. 2 GG im Rahmen der sog. Notstandsgesetze von 1968 ist dem deutschen Gesetzgeber die Möglichkeit eröffnet, den gerichtlichen Rechtsschutz gegen Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses auszuschließen. Von dieser Möglichkeit - eine Verpflichtung dazu bestand und besteht nicht - hat der Gesetzgeber in § 13 G10-Gesetz Gebrauch gemacht. Nach dieser bis heute geltenden Regelung ist „gegen die Anordnung von Beschränkungsmaßnahmen ... und ihren Vollzug ... der Rechtsweg vor der Mitteilung an den Betroffenen nicht zulässig.“ Ob und wann eine solche (nachträgliche) Mitteilung ergeht, ist ungewiss.

Dieser weitgehende Ausschluss des Rechtsschutzes im G10-Gesetz sollte ersatzlos gestrichen werden, damit künftig jeder von nachrichtendienstlichen Eingriffen deutscher Stellen in Art. 10 GG Betroffene uneingeschränkt von dem rechtsstaatlichen Fundamentalrecht auf Anrufung eines unabhängigen Gerichts jederzeit Gebrauch machen kann.

These 4: Die parlamentarischen Kontrollrechte gegenüber den deutschen Nachrichtendiensten sind unzureichend und müssen gestärkt werden. Dabei geht es auch um deren Zusammenwirken mit ausländischen Diensten.

Die im G10-Gesetz vorgesehene parlamentarische Kontrolle durch das Parlamentarische Kontrollgremium (PKG) und die vierköpfige G10-Kommission stellen schon deshalb keinen wirksamen Ersatz für eine gerichtliche Kontrolle dar, weil ihre Mitglieder vom Parlament nach dem Stärkeverhältnis der Fraktionen bestimmt werden. Es dominieren damit in aller Regel die Vertreter der Regierungsmehrheit. PKG und G10-Kommission tagen und verhandeln zudem ausnahmslos geheim in Abwesenheit der Betroffenen. Diese haben vor ihnen nicht die Verfahrensrechte, die ihnen vor unabhängigen Gerichten nach den einschlägigen Prozessordnungen zustünden. Auch der Datenschutzbeauftragte ist „außen vor“.

Nach § 4 PKGrG entscheidet die Bundesregierung selbst, über welche „allgemeine Tätigkeit“ bzw. welche „Vorgänge besonderer Bedeutung“ sie das PKG in Kenntnis setzt. Für die Abgeordneten, die die Handlungen und Unterlassungen von ca. 12.000 Mitarbeitern der deutschen Geheimdienste und deren Abläufe nicht kennen, ist es schwer einzuschätzen, ob die ihnen von der Exekutive vorgetragenen oder verschwiegenen Sachverhalte es tatsächlich rechtfertigen, sie als „Vorgänge besonderer Bedeutung“ oder als „allgemeine Tätigkeit“ zu qualifizieren oder nicht. Deshalb muss zumindest der Inhalt der Unterrichtungspflicht durch Regelbeispiele konkretisiert wer-

den. Diese muss sich auch auf die Tätigkeit anderer Nachrichtendienste im deutschen Hoheitsgebiet oder mit Bezug zu Deutschland beziehen.

Von besonderer Bedeutung ist ferner, dass die Mitglieder der Kontrollgremien endlich ihren Aufgaben entsprechende effektive Arbeitsmöglichkeiten erhalten. Jedem Mitglied sollten zumindest fünf fachlich ausgewiesene Mitarbeiter seiner Wahl zur Verfügung gestellt werden, um den Kontrollaufgaben gegenüber der Exekutive besser gerecht werden zu können. Diese müssen auch an den Sitzungen teilnehmen dürfen.

Es sollte ferner gesetzlich gewährleistet werden, dass sich Mitarbeiter der Nachrichtendienste ohne vorherige Beteiligung ihrer Vorgesetzten uneingeschränkt und unbehindert an die parlamentarischen Kontrollgremien als Ombudstelle (vergleichbar dem Wehrbeauftragten) oder den Bundesdatenschutzbeauftragten wenden dürfen; daraus dürfen ihnen keinerlei beruflichen oder persönlichen Nachteile entstehen.

Die strafrechtlich bewehrte Geheimhaltungspflicht hindert im Grundsatz die Mitglieder der Kontrollgremien, die Regierung öffentlich fundiert zu kritisieren. Die insoweit bestehenden Beschränkungen von öffentlichen Darstellungen über die Gremiumsarbeit und deren Bewertung (vgl. § 10 Abs. 2 und 3 PKGrG) müssen deshalb modifiziert werden. Insbesondere ist sicherzustellen, dass schon ein Minderheitenquorum zur öffentlichen Bewertung der Arbeit des jeweiligen Kontrollgremiums berechtigt.

Die Mitglieder der Kontrollgremien sollten außerdem von ihrer Schweigepflicht im Falle von ihnen bekannt gewordenen Verstößen gegen das Grundgesetz, die Strafgesetze oder gegen von Deutschland abgeschlossene völkerrechtliche Abkommen kraft Gesetzes ausdrücklich entbunden werden. Vorbild für eine solche Regelung könnte die 1951 durch eine interfraktionelle Initiative geschaffene Vorschrift des § 100 Abs. 3 StGB zum Schutz von Bundestagsabgeordneten vor Strafverfolgung wegen Landesverrat bei im Bundestag oder seinen Ausschüssen erfolgter Erwähnung oder Enthüllung von illegalen Staatsgeheimnissen sein, die im Rahmen der Notstandsgesetzgebung 1968 leider wieder beseitigt worden ist. Sie hatte folgenden Wortlaut:

> *„Ein Abgeordneter des Bundestages, der nach gewissenhafter Prüfung der Sach- und Rechtslage und nach sorgfältiger Abwägung der widerstreitenden Interessen sich für verpflichtet hält, einen Verstoß gegen die verfassungsmäßige Ordnung des Bundes oder eines Landes im Bundestag oder in einem seiner Ausschüsse zu rügen, und dadurch ein Staatsgeheimnis öffentlich bekanntmacht, handelt nicht rechtswidrig, wenn er mit der Rüge beabsichtigt, einen Bruch des Grundgesetzes oder der Verfassung eines Landes abzuwehren.“*

These 5: Angesichts der globalen Betätigungsfelder der Nachrichtendienste reicht einzelstaatlicher Grundrechtsschutz nicht aus. Wir benötigen zusätzlich baldmöglichst eine EU-Datenschutzgrundverordnung (DS-GVO), die die Grundrechte im EU-Raum wirksam schützt. Diese Verordnung muss auch für solche Unternehmen gelten, die ihren Sitz außerhalb der EU haben, sich mit ihren Diensten aber an Nutzer und Verbraucher in der EU wenden.

Die im Entwurf der DS-GVO vom November 2011 (Version 56) in Art. 42 ursprünglich vorgesehene sog. Anti-FISA-Klausel ist unverzichtbar und muss entsprechend den Forderungen des EU-Parlaments wieder in diese aufgenommen werden. Diese Klausel war 2012/2013 von der EU-Kommission auf Drängen der US-Regierung und von US-Unternehmen wie Amazon, Google und Facebook aus dem Entwurf gestrichen worden. Eine solche Klausel soll den erforderlichen rechtlichen Rahmen für den Transfer von Daten zwischen EU-Staaten und Drittstaaten (einschließlich der USA) schaffen. Sie soll verhindern, dass Drittstaaten Zugang zu personenbezogenen Daten von EU-Bürgerinnen und Bürgern auf Anforderung eines Nicht-EU-Gerichts oder einer Nicht-EU-Verwaltungsbehörde erhalten oder gewähren, solange dafür keine Genehmigung durch die zuständige EU-Datenschutzbehörde oder des jeweiligen Mitgliedsstaates vorliegt. Diese Regelung muss auch auf entsprechende Aktivitäten der US-amerikanischen National Security Agency (NSA) und anderer Dienste anwendbar sein. Bisher sollen „nachrichtendienstliche Sachverhalte ... nicht dem Anwendungsbereich der DS-GVO“ unterfallen, wie der Parlamentarische Staatssekretär im Bundesinnenministerium Ole Schröder auf eine parlamentarische Anfrage erklärte.[18]

Wenn ein europäisches Tochterunternehmen die Nutzerdaten zum amerikanischen Mutterunternehmen schickt, muss dies als ein Export von Daten qualifiziert werden. Nach EU-Recht darf ein Export von Daten ins EU-Ausland nur erlaubt sein, wenn vom europäischen Unternehmen im Zielland (also z.B. den USA) ein „angemessenes Schutzniveau“ für das Grundrecht auf Datenschutz garantiert werden kann. Diese Anforderungen müssen konkretisiert werden.

Der Rechtsschutz der Bürgerinnen und Bürger vor nationalen Gerichten darf durch eine Harmonisierung des EU-Datenschutzrechts nicht verkürzt werden.

Unternehmen, die in der EU geschäftlich tätig sind und rechtswidrig Informationen an staatliche oder private Stellen weitergeben, müssen mit empfindlichen Strafen belegt werden, die sich zu Abschreckungszwecken an der Höhe des Konzern- oder Unternehmensumsatzes orientieren.

These 6: Die EU sollte mit den USA ein Abkommen über den Schutz des informationellen Selbstbestimmungsrechts sowie der Integrität der IT-Systeme aushandeln und völkerrechtlich wirksam abschließen („EU-US-Datenschutzabkommen“).

Nicht-US-Bürgerinnen und Bürger können sich nicht auf den Schutz des IV. Zusatzartikels der US-Verfassung und bisher ebenso wenig auf Art. 17 des UN-Paktes für bürgerliche und politische Rechte (ICCPR) berufen.[19] Art. 8 der Europäischen Menschenrechtskonvention (EMRK) und Art. 8 der EU-Grundrechte-Charta, die u.a. das Privatleben schützen, das nach allgemeiner Auffassung auch den Datenschutz umfasst, binden weder die USA und noch ihre Nachrichtendienste.

In dem „EU-US-Datenschutzabkommen“ sollte ein individueller Rechtsschutz verankert werden, der allen Bürgerinnen und Bürgern der EU und der USA wechselseitige Klagerechte bei Verstößen gegen das Schutzniveau des IV. Zusatzartikels zur US-Verfassung sowie von Art. 17 ICCPR und Art. 8 EMRK/EuGrCh sowohl vor US-Gerichten als auch vor Gerichten der EU oder ihrer Mitgliedsstaaten einräumt. Ferner soll-

ten sich alle EU-Mitgliedsstaaten und die USA in dem Abkommen verpflichten, für Streitigkeiten über die Auslegung und Anwendung dieses Abkommens und ergänzender völkerrechtlicher Vereinbarungen die Zuständigkeit des Internationalen Gerichtshofs (IGH) in Den Haag nach Art. 36 des IGH-Statuts anzuerkennen.

These 7: Das NATO-Truppenstatut (NTS) und das Zusatzabkommen zum NATO-Truppenstatut (ZA-NTS), in dem eine Vielzahl früherer besatzungsrechtlicher Regelungen Niederschlag gefunden hat, bedürfen einer grundlegenden Revision; die 1993 erreichten Änderungen reichen nicht aus.

(1) Nach Art. 3 ZA-NTS sind die deutschen Behörden und die der Gaststreitkräfte „zu gegenseitiger Unterstützung" verpflichtet. Diese erstreckt sich insbesondere „(a) auf die Förderung und Wahrung der Sicherheit sowie den Schutz des Vermögens der Bundesrepublik, der Entsendestaaten und der Truppen, namentlich auf die Sammlung, den Austausch und den Schutz aller Nachrichten, die für diese Zwecke von Bedeutung sind" sowie „(b) auf die Förderung und Wahrung der Sicherheit sowie auf den Schutz des Vermögens von Deutschen, Mitgliedern der Truppen und der zivilen Gefolge und Angehörigen sowie von Staatsangehörigen der Entsendestaaten, die nicht zu diesem Personenkreis gehören."

Personenbezogene Daten dürfen zwar „ausschließlich zu den im NATO-Truppenstatut und in diesem Abkommen vorgesehenen Zwecken" übermittelt werden. Diese Zwecke sind aber nicht näher definiert. Von Normenklarheit kann keine Rede sein. Sicherungsmaßnahmen sind nicht vorgesehen. Eine weitere Regelung sieht zwar vor, dass „Einschränkungen der Verwendungsmöglichkeiten, die auf den Rechtsvorschriften der übermittelnden Vertragspartei beruhen", „beachtet" werden; Überprüfungs- und Sanktionsmöglichkeiten fehlen jedoch.

Zudem ist nach Art. 3 Abs. 3b ZA-NTS keine Vertragspartei „zur Durchführung von Maßnahmen" verpflichtet, „denen ihre überwiegenden Interessen am Schutz der Sicherheit des Staates oder der öffentlichen Sicherheit entgegenstehen." Die in Art. II NTS normierte Pflicht der Entsendestaaten, ihrer Truppen, ihres zivilen Gefolges, ihrer Mitglieder und deren Angehörigen, das Recht des Aufnahmestaates „zu achten", steht damit im Bereich der nachrichtendienstlichen Zusammenarbeit weithin zur Disposition jeder Vertragspartei, wenn „ihre überwiegenden Interessen am Schutz der Sicherheit des Staates oder der öffentlichen Sicherheit entgegenstehen."

(2) Der/die Bundesbeauftragte für den Datenschutz muss das Recht erhalten, die Beachtung datenschutzrechtlicher Bestimmungen (einschließlich der einschlägigen Grundrechte) sowohl bei den deutschen Nachrichtendiensten als auch auf den den ausländischen Streitkräften überlassenen Liegenschaften (Art. 53 ZA-NTS) zu prüfen und hierüber dem Deutschen Bundestag Bericht zu erstatten.

(3) Die Befugnisse der deutschen Strafverfolgungsbehörden gegenüber den US-Streitkräften und ihrem zivilen Gefolge müssen gestärkt werden. Nach Art. 18 ZA-NTS ist in Deutschland in einem Strafverfahren gegen ein Mitglied einer Truppe oder eines zivi-

len Gefolges (einschl. der Nachrichtendienste) wegen einer in Ausübung des Dienstes begangenen Straftat allein das Recht des betreffenden Entsendestaates, hier also der USA, „maßgebend“. Die „zuständige höchste Behörde“ der USA „kann dem mit der Sache befassten deutschen Gericht“ oder der zuständigen deutschen Behörde (Polizei; Staatsanwaltschaft) „eine Bescheinigung hierüber vorlegen“, die dann von den deutschen Stellen zu beachten ist. Begehen also Bedienstete der US-Streitkräfte oder ihres zivilen Gefolges bei nachrichtendienstlicher Tätigkeit nach deutschen Recht eine Straftat, kann diese nicht von den deutschen Strafverfolgungsbehörden ermittelt und zur Anklage gebracht werden, sofern die US-Behörden nicht zustimmen.

Hier besteht ein erheblicher Revisionsbedarf. Ziel der Revision sollte sein, insbesondere zu gewährleisten, dass die in Deutschland befindlichen ausländischen Truppen und ihr ziviles Gefolge ausnahmslos das deutsche Recht zu beachten haben und dass die zuständigen deutschen Stellen uneingeschränkt befugt sind, auch in den überlassenen Liegenschaften sowie im gesamten Bundesgebiet und im Luftraum darüber die Einhaltung dieser Fundamentalpflicht sowie der weiteren Verpflichtungen effektiv zu überprüfen. Dies muss erst Recht für Straftaten gelten.

These 8: Der mit den USA (sowie dem U.K. und Frankreich) abgeschlossene Aufenthaltsvertrag muss neu verhandelt werden.

Im Aufenthaltsvertrag (AV) vom 23.10.1954 (BGBl 1955 II, S. 253) wird in seinem Art. 1 das in Art. 4 Abs. 2 S. 2 des 1990 aufgehobenen General- oder Deutschland-Vertrags (DV) vom 23.10.1954 zum Ausdruck gebrachte Einverständnis der Bundesrepublik mit der weiteren alliierten Stationierung von Truppen „der gleichen Nationalität und Effektivstärke“ übernommen und bekräftigt; lediglich Erhöhungen der – nicht näher definierten – Effektivstärke werden von der Zustimmung der Bundesregierung abhängig gemacht. Das macht es z.B. äußerst schwierig einzuschätzen und zu kontrollieren, welche Verbände oder „Spezialkräfte“ der US-Streitkräfte und ihres zivilen Gefolges im Bereich der Nachrichtendienste hier bereits stationiert sind oder ggf. neu verlegt werden, welche Aufgabenstellung sie haben und ob diese im Rahmen der NATO-Strukturen oder außerhalb derselben agieren.

Mit anderen Worten: Immer wenn sie sich darauf berufen können, die bisherige „Effektivstärke“ werde nicht geändert, bestehen für die Gaststreitkräfte weite Handlungsräume, ohne dass zwingend die Zustimmung der deutschen Exekutive und des Gesetzgebers eingeholt werden muss. Das zeigte sich jüngst etwa bei der Einrichtung des US-Command in Stuttgart und einer weiteren US-Kommandostelle in Ramstein für Drohnen-Einsätze in Afrika außerhalb von NATO-Strukturen.

Durch Notenwechsel vom 25.9.1990[20] hat die Bundesregierung gegenüber den drei Westmächten ausdrücklich erklärt, dass der Aufenthaltsvertrag „nach der Herstellung der Einheit Deutschlands und dem Abschluss des am 12. September 1990 unterzeichneten Vertrags über die abschließende Regelung in Bezug auf Deutschland in Kraft“ bleibt. Dem deutschen Gesetzgeber ist, soweit ersichtlich, dieser Notenwechsel nicht zur Zustimmung vorgelegt worden. Das ist umso erstaunlicher, als in Art. 3 Abs. 1 AV i.d.F. vom 23.10.1954 ausdrücklich geregelt war und ist, dass der Aufent-

haltsvertrag insgesamt „außer Kraft“ tritt „mit dem Abschluss einer friedensvertraglichen Regelung mit Deutschland oder wenn die Unterzeichnerstaaten zu einem früheren Zeitpunkt übereinkommen, dass die Entwicklung der internationalen Lage neue Abmachungen rechtfertigt.“ Der 2+4-Vertrag vom 15.9.1990 und die damit in Zusammenhang stehenden völkerrechtlichen Vereinbarungen stellten diese „friedensvertragliche Regelung“ im Sinne des Aufenthaltsvertrages dar.

Die durch das parlamentarische Zustimmungsgesetz vom 24.3.1955 innerstaatlich mit Gesetzeskraft und durch die erfolgte Ratifizierung völkerrechtlich wirksam gewordene Regelung in Art. 3 Abs. 1 AV wird durch den Notenwechsel vom 25.9.1990 und die seitherige Staatspraxis fortlaufend missachtet. Dies erschwert die Wahrnehmung der Rechte eines souveränen Staates durch die zuständigen deutschen Staatsorgane.

Jedenfalls in einem Militär-Bündnis wie der NATO, in dem vor allem die dominierende Macht sanktionslos nicht gerade selten Völkerrechtsbrüche begeht (u.a. 2003 Aggressionskrieg gegen Irak[21]; Menschenrechtsverletzungen in Guantanamo[22] und anderen Internierungslagern[23]; gezielte Tötungen von Terrorismus-Verdächtigen ohne rechtsstaatliche Verfahren, nicht selten unter Inkaufnahme erheblicher Schäden für unbeteiligte Zivilpersonen[24]; Steuerung von Drohnen-Angriffen durch US-Kommandoeinrichtungen in Deutschland[25]; CIA-Renditions-Aktionen[26]), muss uneingeschränkt gewährleistet sein und sichergestellt werden, dass deutsche Stellen an solchen gravierenden Rechtsbrüchen nicht mitwirken und diese auch nicht durch „Wegschauen“ oder gar durch aktive Unterstützungsmaßnahmen ermöglichen.

These 9: Die Altlasten des sog. General- oder Deutschland-Vertrages vom 24.10.1954 (DV) müssen beseitigt werden. Alle während seiner Geltung von Deutschland abgeschlossenen geheimen Verträge, Abkommen pp. müssen ausnahmslos gegenüber dem Parlament offengelegt und publiziert werden.

Der General- oder Deutschland-Vertrag ist zwar als solcher seit dem 15.3.1991 nicht mehr in Kraft.[27] Auf seiner Grundlage sind jedoch in den vergangenen Jahrzehnten zahlreiche Regierungs- und Verwaltungsvereinbarungen abgeschlossen worden, die bislang nicht förmlich aufgehoben worden sind. Dabei ging es u.a. um „Überwachungs- und Geheimdienstvorbehalte“, zu denen 1954/55 wie auch in der Folgezeit – zumeist nicht veröffentlichte – völkerrechtlich verbindliche diplomatische Noten ausgetauscht wurden. Dies bezog sich u.a. auf den „Schutz der Sicherheit dieser Streitkräfte“, eine nicht näher definierte und extrem aufnahmefähige Kategorie. Dabei ging es nicht nur um den sog. Notstandsfall[28], sondern u.a. auch konkret um die „Kontrolle von Postsendungen und Überwachung von Fernmeldeverbindungen“ (Art. 5 Abs. 2 S. 3 DV; Art. 4 Abs. 1 und 2 TV) sowie eine Geheimdienst-Regelung, die ergänzend zunächst in Art. 4 Abs. 2 des Truppenvertrages (TV) vom 23.10.1954 (BGBl. II 1954, S. 78-83) und ab dem 1.7.1963 dann u.a. im Zusatzabkommen zum NATO-Truppenstatut vom 3.8.1959 (BGBl. II 1961, S. 1221) verankert wurde. Dies alles liegt weithin im Dunkeln.

Der Deutsche Bundestag sollte deshalb gegenüber der Bundesregierung aktuell darauf dringen und durchsetzen: Alle völkerrechtlichen Verträge, Regierungs- und Verwaltungsabkommen sowie sonstigen Vereinbarungen, die die Bundesrepublik mit den Truppen-Stationierungsländern USA, Frankreich und dem Vereinigten Königreich auf der Grundlage des General-/Deutschland-Vertrages abgeschlossen hat oder die ggf. unabhängig davon die in Art. II des NATO-Truppenstatuts normierte Pflicht der Entsendestaaten, ihrer Truppen, ihres zivilen Gefolges, ihrer Mitglieder und deren Angehörigen, das Recht des Aufnahmestaates Deutschland „zu achten“, einschränken ober beeinträchtigen oder Sonderrechte gewähren, müssen ausnahmslos gegenüber dem Deutschen Bundestag offen gelegt werden. Die Notwendigkeit ihrer Fortexistenz muss jeweils konkret überprüft werden.

Der Text ist ein Originalbeitrag für die vorgänge. Der Beitrag wurde vorab im Onlinemagazin Telepolis veröffentlicht unter: http://www.heise.de/tp/artikel/43/43485/1.html.

DR. DIETER DEISEROTH Jahrgang 1950, ist Richter am Bundesverwaltungsgericht und Mitglied des Beirats der Humanistischen Union. Zahlreiche Veröffentlichungen u.a. zum Friedensgebot des Grundgesetzes (vorgänge Nr. 189), zur völkerrechtlichen Bewertung von Militäreinsätzen und „Humanitären Interventionen“, zum Schutz von Whistleblowern und der Meinungsfreiheit von Redakteuren.

Anmerkungen:

1 Dazu gehört u.a. auch die vom britischen Geheimdienst GCHQ gegen die Zeitung „The Guardian“ mit Drohungen durchgesetzte physische Vernichtung der dort vorhandenen Festplatten mit einem Teil der Kopien der von Edward Snowden gelieferten Datensätze, vgl. dazu Greenwald, Die globale Überwachung, 2014, S. 338 ff.

2 Vgl. dazu die Auswertung der von Snowden enthüllten Daten bei Greenwald, a.a.O., S. 137 ff.; vgl. auch Deiseroth in: ders./Falter (Hrsg.), Whistleblower in der Sicherheitspolitik, 2014, S. 11 ff.

3 Vgl. Greenwald, a.a.O., S. 142 ff.

4 Der in seiner ursprünglichen Fassung am 25.10.1978 in Kraft getretene FISAct (Fundstelle: U.S. Code Title 50, Chapter 36 §§ 1801 ff.) diente seinerzeit dem Ziel, die von der Exekutive allein auf die „inherent power“ des US-Präsidenten gestützten Abhöranordnungen zu nachrichtendienstlichen Zwecken legislativ einzuhegen; vgl. dazu u.a. Egbert Beier, Geheime Überwachungsmaßnahmen zu Staatssicherheitszwecken außerhalb des Gesetzes zur Beschränkung von Art. 10 GG, 1988, S. 134 ff. m.w.N. Der Foreign Intelligence-Amendment Act (FISAA) von 2008 weitete die Befugnisse der US-Nachrichtendienste im Ausland deutlich aus, insbesondere um die Daten von Unternehmen in den USA besser abschöpfen zu können.

5 „USA-Patriot“ steht für: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act; abrufbar unter: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm (aufgerufen am 16.11.2014).
6 Vgl. Reuters/JW v. 14.10.2013, S. 1.
7 Vgl. dazu u.a. Gusy, § 2 BND-Gesetz in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, S. 1278.
8 Vgl. dazu die sog. Lotus-Entscheidung des Ständigen Internat. Gerichtshofs v. 7.9.1927 (PCIJ, Series A., No. 10, 1927).
9 Für Kriegszeiten vgl. aber Art. 39 Abs. 3 des I. Genfer Zusatzprotokolls v. 12.12.1977 („existing generally recognized rules of international law applicable to espionage“).
10 Vgl. dazu u.a. Berber, Völkerrecht, Bd. II, 2. Aufl. 1969, S. 147; Langkau, Völker- und landesrechtliche Probleme der Kriegs- und Friedenspionage, Diss. Würzburg, 1971, S. 84 ff., 171 ff.; Doehring, ZRP 1995, 293 (295) m.w.N.; Gusy, NZWehrR 1984, 187; Beier, Geheime Überwachungsmaßnahmen zu Staatssicherheitszwecken außerhalb des Gesetzes zur Beschränkung von Art. 10 GG,1988, S. 78 ff. m.w.N.
11 Abrufbar unter: http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf
12 Vgl. etwa das Verfahren Aftergood vs. CIA, Case No. 01-2524, D.D.C., 9.2.2005; dazu Rahul Sagar, Das missbrauchte Staatsgeheimnis, in: Wikileaks und die Folgen, 2011, S. 201, 206 f.
13 Das BVerwG sieht „Nachteile“ für „das Wohl des Bundes oder eines Landes“, die zur Verweigerung der Vorlage von Akten durch eine oberste Bundes- oder Landesbehörde nach § 99 Abs. 1 S. 2 VwGO berechtigten, schon dann als gegeben an, „wenn und soweit die Bekanntgabe des Akteninhalts die künftige Erfüllung der Aufgaben der Sicherheitsbehörden einschließlich deren Zusammenarbeit mit anderen Behörden erschweren würde“, vgl. Beschluss v. 18.2.2014 - BVerwG 20 F 10.13 - juris Rn. 5 m.w.N.
14 Iljia Trojanow, Die Kollateralschäden des kalten Bürgerkriegs, NZZ v. 2.8.2013, abrufbar unter http://www.nzz.ch/meinung/uebersicht/die-kollateralschaeden-des-kalten-buergerkriegs--1.18126416.
15 Vgl. dazu u.a. Deiseroth in: ders./Falter, Whistleblower in der Sicherheitspolitik, a.a.O., S. 8 ff.
16 Vgl. dazu u.a. Deiseroth, Societal Verification, 3. Aufl. 2010.
17 Vgl. dazu u.a. Hoffmann-Riem, Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22.5.2014, S. 15 m.w.N., abrufbar unter: https://netzpolitik.org/wp-upload/mat_a_sv-2-1neu-pdf-data.pdf (aufgerufen am 14.11.2014); Szcekalla, DVBl. 2014, 1108 (1110) m.w.N.
18 Verhandlungen des Deutschen Bundestages, 17. Wahlperiode, 249. Sitzung am 26.6.2013, S. 3187.
19 Vgl. u.a. Deiseroth in: ders./Falter, Whistleblower in der Sicherheitspolitik, 2014, S. 19.
20 BGBl. 1990 II 1390.
21 Vgl. dazu u.a. BVerwG, Urteil v. 21.6.2005 - 2 WD 12.04 -, NJW 2006, 77 ff. m.w.N.
22 Vgl. Amnesty International Schweiz, Dossier Guantánamo, abrufbar unter: http://www.amnesty.ch/de/themen/sicherheit-und-menschenrechte/guantanamo (10.9.2013).
23 Florian Diekmann, Tod von Terrorgefangenen: US-Justiz ermittelt gegen CIA-Agenten, Spiegel Online v. 1.7.2011, abrufbar unter: http://www.spiegel.de/politik/ausland/tod-von-terrorgefangenen-us- justiz-ermittelt-gegen-cia-agenten-a-771694.html.
24 Peter Rudolf/Christian Schaller, „Targeted Killing“. Zur völkerrechtlichen, ethischen und strategischen Problematik gezielten Tötens in der Terrorismus- und Aufstandsbekämpfung, Studie im Auftrag der SWP, Berlin 2012, abrufbar unter http://www.swp-berlin.org/fileadmin/contents/products/studien/2012_S01_rdf_slr.pdf.
25 NDR-Panorama v. 30.5.2013, abrufbar unter: http://daserste.ndr.de/panorama/archiv/2013/ramstein109.html und SZ v. 30.5.2013.
26 Vgl. Parl. Versammlung des Europarates und Berichte seines Rapporteurs Dick Marty von 2006 und 2007, in: http://assembly.coe.int/ASP/Press/StopPressView.asp?ID=1924 (10.9.2013).
27 Vgl. BGBl 1990 II, S. 1386, hier S. 1387, Ziff. 1.

28 In Art. 5 Abs. 3 S. 1 DV; vgl. dazu u.a. den mit Bundeskanzler Adenauer ausgehandelten Brief der Außenminister der drei Westmächte v. 23.10.1954, veröffentlicht u.a. in: Foschepoth, Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik. Göttingen 2012; 4. durchgesehene Auflage 2014, Dok. Nr. 1b S. 287f.