Humanistische Union

Deutsche Rechtspositionen zur Überwachungsaffäre

aus: vorgänge Nr. 206/207 (Heft 2-3/2014), S. 7-21

(Red.) Am 3. April 2014 nahm der 1. Parlamentarische Untersuchungsausschuss des 18. Deutschen Bundestags zur NSA-Affäre seine Arbeit auf. Ziel des Ausschusses ist es, den Umfang der mutmaßlichen Ausforschungen, die mögliche Beteiligung deutscher Behörden sowie die technisch wie rechtlich gebotenen Maßnahmen für einen besseren Schutz des Fernmeldegeheimnisses zu ermitteln. Der Ausschuss ist nicht nur Ausdruck des parlamentarischen Informations- und Kontrollanspruchs, er ist auch für die Öffentlichkeit ein wichtiges Instrument, um die zahlreichen Enthüllungen aus den Snowden-Dokumenten einzuordnen und das Vertrauen in die rechtsstaatliche Arbeit der Sicherheitsbehörden wiederherzustellen.

Zum Auftakt führte der Untersuchungsausschuss mehrere Sachverständigenanhörungen durch, in denen rechtliche und technische Rahmenbedingungen der geheimdienstlichen Überwachungstätigkeit erörtert wurden.(1) Der vorliegende Beitrag fasst die verfassungsrechtlichen Gutachten der früheren Richter des Bundesverfassungsgerichts, Prof. Dr. Hans-Jürgen Papier und Prof. Dr. Wolfgang Hoffman-Riem, sowie von Prof. Dr. Matthias Bäcker zusammen: Welche Abhörmaßnahmen sind den deutschen Geheimdiensten erlaubt? Welche faktischen und rechtlichen Probleme gibt es dabei? Was muss, kann und sollte die Bundesregierung zum Schutz des Fernmeldegeheimnisses unternehmen.

Massenhafte Erhebung und Speicherung von Telekommunikationsdaten - in Deutschland zulässig?

Die Frage, ob eine verdachtsfreie Massenspeicherung von Telekommunikationsdaten (wie beim Abhörprogramm Mystic) in Deutschland zulässig wäre, lässt sich eigentlich einfach beantworten: eine solche Praxis wäre weder mit der Verfassung noch mit dem Fachrecht der deutschen Geheimdienste vereinbar – eigentlich. Die Einschränkung ist in doppelter Hinsicht notwendig, denn zum einen betreibt der Bundesnachrichtendienst (BND) seit Jahren eine strategische Überwachung der Auslandskommunikation, bei der massenhaft Kommunikationsdaten ausgewertet werden. Darüber hinaus hat die Bundesregierung inzwischen eingeräumt, dass der BND eine noch umfangreichere Überwachung der Auslandskommunikation vornimmt, die offenbar an den deutschen Gesetzen vorbei erfolgt. (Zu beiden Ausnahmen später mehr.)

Die verfassungsrechtlichen Grenzen der massenhaften Erhebung von Telekommunikationsdaten skizziert Papier in seiner Stellungnahme, angelehnt an die Entscheidung des Bundesverfassungsgerichts zur sog. Vorratsdatenspeicherung vom 2. März 2010.(2) Die wichtigsten in diesem Urteil formulierten Kriterien für eine verfassungskonforme Massenspeicherung von Verkehrsdaten (Metadaten) gelten auch für die Arbeit der Geheimdienste, so Papier (S. 3ff.):

- es werden nur Verkehrs- bzw. Metadaten, nicht die Inhalte der Kommunikation erfasst
- die Speicherung erfolgt nicht bei staatlichen Stellen; staatliche Behörden haben keinen direkten Zugriff auf die Daten

- ein besonders hoher Standard der Datensicherheit bei den speichernden Firmen ist gesetzlich zu gewährleisten
- die Daten dürfen nur für „überragend wichtige Aufgaben des Rechtsgüterschutzes“ genutzt werden
- der Abruf der Daten ist nur auf richterliche Anordnung zulässig
- eine richterliche Kontrolle der Datenverwendung sowie ein effektiver Rechtsschutz für die Betroffenen ist zu garantieren.

Für den geheimdienstlichen Umgang mit solchen Daten hieße das: Die Daten dürfen nur zur Abwehr von „Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder [zur] Abwehr einer gemeinen Gefahr“ (Papier, S. 4) genutzt werden. Dabei müssen tatsächliche Anhaltspunkte auf das Bestehen einer konkreten Gefahr vorliegen. „Eine Verwendung der vorsorglich gespeicherten Daten durch die Nachrichtendienste dürfte daher in vielen Fällen ausscheiden, wenn und weil diese vorrangig im Bereich der Vorfeldaufklärung tätig sind.“ (Papier, S. 5) Damit ist ein relativ enger Bereich umrissen, in dem eine geheimdienstliche Nutzung von vorrätig gespeicherten Kommunikationsdaten zulässig wäre. Da jedoch alle anderen, oben aufgezählten Verfahrenssicherungen für eine solche Speicherung nicht erfüllt sind, dürfen deutsche Geheimdienste (genauso wie die Strafverfolgungsbehörden) von Verfassung wegen Kommunikationsdaten verdachtsunabhängig weder erheben, speichern noch nutzen.

Neben den verfassungsrechtlichen Grenzen sieht auch das **Fachrecht der Geheimdienste** – einmal abgesehen von der strategischen Auslandsüberwachung durch den BND (dazu unten mehr) – keine Möglichkeiten für eine verdachtsunabhängige Erhebung oder Speicherung von Kommunikationsdaten vor. Mit den fachgesetzlichen Vorgaben befasst sich ausführlich die Stellungnahme von Bäcker. Sein Gutachten geht auf die Regeln zur Erhebung, Speicherung und Verwendung sowie Weitergabe von Kommunikationsdaten durch BND und Bundesamt für Verfassungsschutz (BfV) ein. Im Einzelnen handelt es sich um folgende Befugnisse:(3)

- die gezielte Überwachung von Kommunikationsinhalten nach § 3 Abs. 1 G10-Gesetz (G10) durch BND und BfV
- den Abruf von Verkehrsdaten bei den Diensteanbietern (sofern diese dort vorliegen)(4) nach § 8a Abs. 2 Satz 1 Nr. 4 BVerfSchG bzw. § 2a BNDG
- die strategische Überwachung der grenzüberschreitenden Kommunikation durch den BND nach § 5 G10.

Die genannten Rechtsgrundlagen sind in vielerlei Hinsicht kritikwürdig, Bäcker listet in seiner Stellungnahme eine ganze Reihe problematischer bzw. verfassungswidriger Einzelbestimmungen auf. So stützt sich § 3 Abs. 1 G10 auf einen Katalog von Straftaten, bei denen der Verdacht auf entsprechende Vorbereitungshandlungen eine Überwachungsmaßnahme begründen kann. Dieser Katalog enthält selbst sogenannte Vorfeldstraftaten (etwa die Beteiligung an einer terroristischen Vereinigung gem. § 129a StGB), wodurch es zu einer „doppelten Vorverlagerung“ kommt, indem bereits die Planung einer Vorfeldstraftat zum Anlass der Kommunikationsüberwachung wird. Außerdem enthält der Katalog strafrechtlich gesehen auch Bagatelldelikte (etwa die Fortführung eines verbotenen Vereins nach § 20 Abs. 1 VereinsG), bei denen eine TK-Überwachung unverhältnismäßig erscheint. Die Erhebung von Verkehrsdaten durch den Verfassungsschutz wiederum knüpft an sehr allgemein gehaltene Schutzgüter (wie die auswärtigen Belange der Bundesrepublik oder den Gedanken der Völkerverständigung) an, deren „Gefährdung“ sich kaum präzise bestimmen lässt. Die Verkehrsdatenerhebung durch BND und BfV sei deshalb nur dann verfassungskonform, wenn eine „Gefährdungslage im Einzelfall [vorliegt], die zumindest ansatzweise nach Art, Ort, Zeit und Beteiligten konturiert werden kann. Zudem muss es sich um eine schwerwiegende

Gefährdung handeln.“ (Bäcker, S. 5f.)(5)

Bei aller Kritik gilt dennoch: „Trotz ihrer erheblichen Weite ermöglichen die Ermächtigungen zu gezielten Datenerhebungen und die Folgeermächtigungen jedoch keine anlasslose und flächendeckende Datenbevorratung für nachrichtendienstliche Zwecke.“ (Bäcker, S. 8) Zum einen muss sich die Überwachung der Kommunikationsinhalte wie der Verkehrsdaten auf einen bestimmten – wenn auch nur vage konturierten – Gefahrenanlass beziehen. Sie darf sich nur gegen Personen (sowie deren Nachrichtenmittler_innen) richten, welche diese mögliche Gefahr fördern. Die geheimdienstlichen Überwachungsmaßnahmen sind auf bestimmte Personenkreise zu beschränken. Darüber hinaus verlangen die gesetzlichen Vorschriften zur Speicherung, „die erhobenen Daten unverzüglich und danach turnusmäßig auf ihre nachrichtendienstliche Relevanz zu prüfen. Fällt diese Prüfung negativ aus, so sind die Daten zu löschen. Daten dürfen darum nicht schon deshalb bevorratet werden, weil sie irgendwann einmal relevant werden könnten.“ (ebd.)

Ausnahme 1: Die strategische Überwachung der grenzüberschreitenden Kommunikation

Eine große Ausnahme von allem bisher Gesagten stellt die strategische Überwachung der grenzüberschreitenden Kommunikation durch den BND nach § 5 G 10-Gesetz dar. Sie wurde ursprünglich zu Zeiten des Kalten Krieges eingeführt, vorgeblich um einen bevorstehenden bewaffneten Angriff aus dem Ostblock frühzeitig zu erkennen. Dafür durfte der BND die Telekommunikation von Westdeutschland ins Ausland bzw. aus dem Ausland nach Westdeutschland mit Hilfe bestimmter Schlüsselbegriffe auf entsprechende Hinweise durchsuchen.(6) Nach dem Ende des Ost-West-Konflikts und dem Ausbau der Europäischen Union war diese Gefahr eines militärischen Angriffs auf Deutschland eigentlich obsolet. Dennoch wurde die strategische Fernmeldeaufklärung des BND nicht abgeschafft, sondern mit dem Verbrechensbekämpfungsgesetz vom 28. Oktober 1994 auf neue Gefahrenbereiche erweitert. Seitdem darf der BND die grenzüberschreitende Kommunikation auch auf Hinweise zu terroristischen Anschlägen, auf den Handel mit Kriegswaffen und militärischen Rüstungsgütern, die Einfuhr von Betäubungsmitteln und Geldfälschungen bzw. Geldwäsche durchsuchen. Anlässlich der Erweiterungen der strategischen Fernmeldeüberwachung im Jahre 1994 befasste sich auch das Bundesverfassungsgericht mit dieser Form der großflächigen TK-Überwachung und befand sie, abgesehen von einigen Nachbesserungen bei den Regeln zur Datenweitergabe und der Zweckbindung der erhobenen Daten, im Wesentlichen für verfassungskonform.(7)

Daraus zu folgern, dass die heutige Rechtslage bzw. Praxis der strategischen Fernmeldeaufklärung verfassungskonform sei, wäre jedoch falsch, betont Bäcker in seiner Stellungnahme (s.S. 9ff.). Einerseits haben sich seit der Entscheidung des Bundesverfassungsgerichts die rechtlichen Grundlagen nochmals geändert, vor allem aber auch die technischen Bedingungen der Telekommunikation und ihrer Überwachung. Das zeigt sich bei all jenen gesetzlichen Bestimmungen, die die Überwachungstätigkeit in ihrem Ausmaß begrenzen sollen:

- Das Gesetz sieht eine Auswahl an Ländern bzw. Zielregionen vor, deren Kommunikationsverkehr von und nach Deutschland überwacht werden darf. Zudem soll die Überwachung durch die Verwendung einer von der G 10-Kommission zu genehmigende **Liste von Suchwörtern** eingegrenzt werden. Nur die „Treffer“-Nachrichten, in denen sich die Suchwörter finden, werden von Mitarbeiter_innen des BND gesichtet und bearbeitet. Wie wenig diese Verfahrensvorkehrungen helfen, die „Trefferliste“ einzugrenzen, zeigen die Zahlen aus 2010: damals gaben die Filter des BND rund 37 Millionen E-Mails als Treffer für die gesuchten Hinweise aus. In diesem Fall handelte es sich bei den meisten Nachrichten wohl um Spam,(8) das grundrechtliche Problem bleibt aber das gleiche.
- Die weit gefassten Anwendungsbereiche (s.o.), bei denen die strategische Überwachung angewandt

werden darf, setzen keine konkrete Gefahr voraus, es reicht eine **„allgemeine Bedrohungslage“.** „Hinsichtlich der meisten Gefahrenbereiche ermöglicht das G 10 dem BND deshalb eine permanente Überwachungstätigkeit, da stets mit entsprechenden Gefährdungen zu rechnen ist.“ (Bäcker, S. 10)

- Die Einschränkung, dass der BND **nur grenzüberschreitende, internationale Kommunikationsvorgänge** überwachen darf, ist angesichts der Übertragungswege des Internets schwierig umzusetzen. Jede netzgestützte Kommunikation (IP-Telefonie, E-Mail, Chat ...) wird nach den Routing-Regeln der Zugangs- und Netzbetreiber des Internets übermittelt. Dabei werden regelmäßig Nachrichten über ausländische Verbindungen geleitet, selbst wenn sich Absender_in und Empfänger_in in Deutschland befinden. „Auch wenn etwa ein Übertragungskabel überwacht wird, das vom Inland ins Ausland führt, kann ein erheblicher Teil der übertragenen Telekommunikation letztlich für das Inland bestimmt sein.“ (Bäcker, S. 11) Das Vorliegen einer internationalen Kommunikationsbeziehung müsste also anhand der Kommunikationsteilnehmer_innen geprüft werden. Das ist aber ebenso schwer zu ermitteln, denn der Name eines E-Mail-Accounts gibt weder Aufschluss über dessen Inhaber_in noch dessen/deren Aufenthaltsort.
- Nach der derzeit geltenden Gesetzesfassung darf der BND alle Telekommunikationswege überwachen, egal ob die Nachrichten via Satellit, Telefonleitung, Internet oder Funk ausgetauscht werden. (In der vom Bundesverfassungsgericht geprüften Fassung war die Befugnis noch auf die nicht-leitungsgebundene Kommunikation beschränkt.) Einschränkend sieht das Gesetz vor, dass eine Überwachung nur zulässig sei, „soweit eine **gebündelte Übertragung** erfolgt“. Das trifft heute jedoch, abgesehen von der „letzten Meile“ zum Hausanschluss, auf praktisch alle Übertragungswege zu und stellt keinerlei Beschränkung mehr dar.
- Schließlich soll die Überwachung dadurch begrenzt werden, dass der BND maximal 20 Prozent der vorhandenen **Übertragungskapazitäten** überwachen darf. Die Begrenzung orientiert sich wohlgemerkt nicht am tatsächlichen Nachrichtenaufkommen, sondern an der Kapazität des überwachten Kanals. Die Übertragungskapazitäten des Internets sind i.d.R. auf das Mehrfache des normalen Datenaufkommens ausgelegt, um Übertragungsprobleme und Netzausfälle in Stoßzeiten zu vermeiden. So verfügt der größte deutsche Internetknoten DE-CIX über eine Kapazität von max. 10 TBit/s, im Tagesdurchschnitt werden dessen Leitungen jedoch mit weniger als 2 TBit/s ausgelastet (Zahlen nach Bäcker, S. 13). Dem Gesetzeswortlaut zufolge dürfte der BND zu normalen Zeiten also sämtlichen Datenverkehr an diesem Knoten auswerten. Weiterhin ist unklar, auf welche Stufe der Filterung und Bearbeitung sich die Vorgabe von max. 20 Prozent der Daten bezieht, ob der BND also zuvor bereits inländische Kommunikationsverbindungen herausrechnen darf oder nicht (ebd.).
- § 5 Abs. 2 Satz 2 G 10-Gesetz verbietet die Verwendung von formalen Suchbegriffen, mit denen sich **einzelne Telekommunikationsanschlüsse** in den Datenströmen identifizieren lassen. Damit soll der Gefahr einer gezielten Überwachung einzelner Personen begegnet werden. Dieses Verbot schützt vereinfacht gesagt nur die klassische Telefonie und den Mobilfunk, da es sich auf Rufnummern bzw. vergleichbare Zugangsadressen (gem. § 2 Nr. 10 TKÜV) bezieht. Bei allen internetgestützten Kommunikationsformen (etwa E-Mails) werden die Teilnehmer_innen jedoch durch Benutzerkennungen auf Dienstebene identifiziert (etwa den E-Mail-Account bzw. die Mailadresse), weshalb dieses Identifizierungsverbot hier nicht greift. „Wird der Wortlaut von § 5 Abs. 2 Satz 2 G 10 ernst genommen, so verbietet die Norm darum nicht, den Datenstrom gezielt anhand bestimmter E-Mail-Adressen auszuwerten, obwohl die grundrechtliche Gefährdungslage nicht weniger schwer wiegt als etwa bei einer Auswertung mittels bestimmter Telefonnummern.“ (Bäcker, S. 14) Das Verbot der Identifizierung von Kommunikationsteilnehmer_innen gilt zudem laut Gesetz nur für deutsche Teilnehmer_innen – obwohl das Fernmeldegeheimnis gleichermaßen für Deutsche wie Ausländer_innen gilt; ein klarer Verstoß gegen den Grundsatz der Gleichbehandlung.

Die gesetzlichen Grundlagen zur strategischen Fernmeldeüberwachung ebenso wie die Praxis des BND sind also in vielerlei Hinsicht bedenklich. Umso bedauerlicher, dass eine vom Berliner Rechtsanwalt Niko Härting angestrengte Klage vor dem Bundesverwaltungsgericht scheiterte und die geplante

Verfassungsbeschwerde nicht zustande kam.(9)

Ausnahme 2: Die reine Auslandsüberwachung des BND

Im Sommer 2013 zitierte der Spiegel aus den Snowden-Dokumenten, wonach der BND allein im Dezember 2012 rund 500 Millionen Metadatensätze (Verkehrsdaten) an die NSA übermittelt habe. Der BND versicherte zugleich, dass vor der Weitergabe die zu deutschen Staatsbürgern gehörenden Daten herausgefiltert worden seien und der Austausch auf gesetzlicher Grundlage (nach BND- und G10-Gesetz) erfolge. Daran sind Zweifel angebracht. Allein schon die Größenordnung, in der hier Kommunikationsdaten erhoben und ausgetauscht wurden, steht in absolutem Widerspruch zu dem, was nach dem G10-Verfahren erhoben und ausgetauscht wird und sich in den jährlichen Berichten des Parlamentarischen Kontrollgremiums wiederfindet: Für das Jahr 2011 (das letzte bisher veröffentliche Berichtsjahr) genehmigte die G 10-Kommission für BfV, BND und MAD insgesamt 156 Maßnahmen zur gezielten Überwachung von Kommunikationsinhalten (nach § 3 G 10). Im gleichen Zeitraum erfasste der BND bei der strategischen Überwachung der grenzüberschreitenden Kommunikation insgesamt 2.875.000 Kommunikationsvorgänge (vorwiegend E-Mails), von denen letztendlich 260 Mitschnitte als nachrichtendienstlich relevant eingestuft und von Mitarbeiter_innen ausgewertet wurden. Dem Bericht zufolge wurden in 2011 keine (sprich: 0) Daten aus der strategischen Überwachung an ausländische Stellen übermittelt. Diesen Zahlen stehen die oben genannten 500 Millionen Datensätze gegenüber, die der BND innerhalb eines Monats an die NSA übergeben haben soll.

Dass der BND bei der hier erwähnten Datenerhebung und -weitergabe am gesetzlich festgelegten Verfahren vorbei operiert, legt auch ein Beitrag von Bertold Huber, dem stellvertretenden Vorsitzenden der G10-Kommission, nahe.(10) Er berichtet im August 2013 erstmals darüber, dass der BND neben der strategischen Fernmeldeaufklärung, die „nur“ die grenzüberschreitende Kommunikation betrifft, offenbar in weit größerem Ausmaß auch reine Auslandskommunikationen (etwa innerafghanische Gespräche) überwacht. Diese Überwachungstätigkeit „[unterliege] insoweit nicht den Regularien des G 10, so dass eine Kontrollkompetenz der G 10-Kommission nicht gegeben ist.“(11) Diese Vermutung bestätigte die Bundesregierung kurze Zeit später in ihrer Antwort auf eine parlamentarische Anfrage von Bündnis 90/Die Grünen.12 Demnach rechtfertigen BND bzw. Bundesregierung diese Überwachung der Auslandskommunikation mit **Verweis auf die allgemeinen Aufgabenbestimmungen und Generalbefugnisse** in § 1 Abs. 2 und § 2 Abs. 1 Nr. 4 BND-Gesetz.(13) Diese „Rechtsauffassung“ der Bundesregierung ist sowohl in verfassungsrechtlicher wie fachrechtlicher Sicht ein Hohn für die bundesdeutsche Rechtsordnung und wurde von den Sachverständigen im Untersuchungsausschuss scharf angegriffen. Die Begründungen im Einzelnen:

Das Fernmeldegeheimnis (Artikel 10 Grundgesetz) ist **kein sogenanntes „Deutschen-Grundrecht“**, d.h. es gilt für deutsche Staatsbürger_innen wie Ausländer_innen gleichermaßen. Einschränkungen des Fernmeldegeheimnisses für Ausländer_innen bedürfen daher genauso einer gesetzlichen Ermächtigung (die geeignet, erforderlich und verhältnismäßig sein muss) wie die Überwachung von Deutschen.

Der **Schutzbereich des Fernmeldegeheimnisses** gilt zudem – jedenfalls für deutsche Behörden – über die Staatsgrenze hinaus. Es mag zwar sein, dass das Grundrecht wie sein Vorläufer, das Postgeheimnis, ursprünglich auf das jeweilige Staatsgebiet bezogen waren – Pakete, Briefe oder Telefonate waren i.d.R. auch territorial gebunden. Für die digitale, internetgestützte Kommunikation gilt das jedoch nicht mehr (s.o.). Bei vielen Internet-Kommunikationsanbietern handelt es sich um internationale Firmen, deren technische Infrastruktur weltweit verteilt ist. So kann bereits das Einloggen in den eigenen E-Mail-Account zum grenzüberschreitenden Datenverkehr führen. Die Unterscheidung zwischen Inlands-, grenzüberschreitender und reiner Auslandskommunikation ist aus technischer Sicht kaum noch sachgerecht. Hoffmann-Riem betont daher, dass das Fernmeldegeheimnis heute angemessen nur noch als grenzüberschreitendes, territorial nicht gebundenes Grundrecht anzuwenden ist: „Rechtsstaatlicher

Freiheitsschutz gilt dem Kommunikationsvorgang selbst. Der Schutz würde teilweise leerlaufen, wenn er davon abhinge, ob ein Kommunikationsvorgang mehr oder minder unvorhersehbar/zufällig über Leitungen in deutschen oder in nichtdeutschen Gebieten abgewickelt wird.“ (Hoffmann-Riem, S. 10) Mit anderen Worten: „Sofern beide Endpunkte des Telekommunikationsverkehrs im Ausland liegen, sind die den Eingriff in das Telekommunikationsgeheimnis vornehmenden deutschen Behörden grundsätzlich ebenfalls an Art. 10 GG gebunden; der räumliche Schutzumfang des Fernmeldegeheimnisses ist also nicht auf das Inland begrenzt“ (Papier, S. 7).

Daran ändert sich auch nichts, wenn die **deutschen Behörden im Ausland tätig** werden. Einerseits werden die erhobenen Daten sowieso bei deutschen Stellen (z.B. in Pullach, dem Sitz des BND) verarbeitet. Viel grundsätzlicher gilt hier jedoch Artikel 1 Abs. 3 Grundgesetz: Unsere Verfassung bindet die deutsche Staatsgewalt an die Grundrechtsordnung als „unmittelbar geltendes Recht“. Diese Bindung hat keine territorialen Grenzen. Wenn deutsche Behörden wie der BND im Ausland operieren, sind sie dennoch zur Einhaltung der Grundrechte verpflichtet. „Die Grundrechte binden in ihrem sachlichen Geltungsumfang die deutsche öffentliche Gewalt auch, soweit Wirkungen ihrer Betätigung außerhalb des Hoheitsbereichs der Bundesrepublik Deutschland eintreten.“ (BVerfGE 57, 9 (23) zitiert nach Hoffmann-Riem, S. 10) Der allgemeinen Aufgabenbestimmung des BND fehlen darüber hinaus alle Merkmale einer gesetzlichen Regelung für einen verfassungskonformen Grundrechtseingriff:

Sie bietet keine effektive Begrenzung der staatlichen Überwachungstätigkeit. Folgt man der Rechtsauffassung der Bundesregierung, dürfte der BND auf dieser „Rechtsgrundlage“ so viele Kommunikationsvorgänge überwachen, wie er technisch realisieren könnte – eine flächendeckende Überwachung wäre nicht ausgeschlossen.

- Es gäbe keinerlei Vorkehrungen gegen das Abhören der Intimsphäre, der Schutz des Kernbereichs privater Lebensgestaltung (der sich aus der Menschenwürdegarantie ableitet) wäre nicht gewährleistet;
- Es fehlt die Prüfung darauf, ob die Abhörmaßnahmen in einem angemessenen Verhältnis zu den konkret damit verfolgten Zwecken stehen, der Grundrechtseingriff angemessen ist.
- Es fehlen jegliche verfahrenssichernden Maßnahmen (Wer darf solche Maßnahmen bspw. anordnen?) und es gibt keinerlei Benachrichtigung oder gar Rechtsschutzverfahren für die Betroffenen.
- Es fehlt dem BND-Gesetz der notwendige Hinweis auf die Einschränkung des Fernmeldegeheimnisses durch die §§ 1 und 2 (Verletzung des Zitiergebotes).

Bleibt am Ende nur die Frage: Wie ist diese rechtswidrige Überwachungspraxis des BND zu stoppen, und wer macht es?

Datenaustausch mit ausländischen Geheimdiensten

Nicht nur die Mitglieder der *Five Eyes-Allianz*, sondern auch der bundesdeutsche BND steht im Verdacht, die Grenzen nationaler Überwachungsmöglichkeiten dadurch zu umgehen, dass eigene Staatsbürger_innen von befreundeten Diensten abgehört werden, die die Ergebnisse ihrer Überwachung dann für ihre Partnerdienste zur Verfügung stellen. Eine derartige Praxis wird vor allem durch zwei Umstände ermöglicht: Erstens fallen die Unterschiede in den Überwachungsgesetzen westlicher Staaten viel geringer aus, als gemeinhin angenommen wird.(14) Eine zentrale Gemeinsamkeit besteht in der oben für den BND beschriebenen Unterscheidung zwischen der Überwachung eigener Staatsbürger_innen (in einem vergleichsweise begrenzten Umfang zulässig) und der Überwachung von Ausländern (im Vergleich nahezu unbeschränkt möglich). Diese Ungleichbehandlung wird beim Ringtausch ausgenutzt: Personen, die der eine Geheimdienst nicht überwachen darf, darf der andere überwachen und umgekehrt.(15) Hinzu kommt

zweitens, dass die gesetzlichen Vorschriften zum internationalen Datenaustausch zwischen den Geheimdiensten sehr vage sind, sofern es überhaupt Regelungen dafür gibt.

Aus verfassungsrechtlicher Sicht scheint die Sache eindeutig: Papier erinnert in seiner Stellungnahme daran, dass die Erfassung, die Speicherung, die Auswertung und der Abgleich sowie die Übermittlung von Daten an Dritte jeweils eigene Grundrechtseingriffe darstellen. Für den internationalen Datenaustausch heißt das: sofern es sich um Kommunikationsdaten handelt, die dem Schutz von Artikel 10 GG unterliegen, hat sich nicht nur die Erhebung (das „Abhören"), sondern haben sich deutsche Behörden bei allen Schritten der Datenverarbeitungskette an die Voraussetzungen zum Eingriff in das Fernmeldegeheimnis zu halten. „Dieser **Grundsatz des fortbestehenden Schutzes durch Art. 10 GG** verlangt auch eine Kennzeichnung der durch einen ersten Eingriff in das Telekommunikationsgeheimnis erhaltenen Daten." (Papier, S. 2 mit Verweis auf BVerfGE 100, 313 (319); 125, 260 (309f.)) Eine Weitergabe genauso wie eine Entgegennahme von Daten, die mittels Telekommunikationsüberwachung gewonnen wurden, darf daher nur stattfinden, sofern dafür eine ausdrückliche gesetzliche Regelung besteht. Die muss normenklar und bereichsspezifisch sein (s. Papier, S. 9) und dem Maßstab der Verhältnismäßigkeit für Eingriffe in Artikel 10 GG genügen. Im Klartext: Deutsche Sicherheitsbehörden, allen voran der BND, dürften Daten ausländischer Geheimdienste, die aus Telefonüberwachungen gewonnen wurden, nur dann annehmen und verarbeiten, wenn die Erhebung den Schutzmaßstäben von Artikel 10 GG (und den sie ausführendem deutschen Fachrecht) genügt.

Das klingt gut – dürfte im geheimdienstlichen Alltag aber kaum so eingehalten werden. Wenn der BND etwa Informationen von der NSA erhält, werden diese keine Hinweise darauf enthalten, unter welchen Voraussetzungen und mit welchen Mitteln sie von der NSA erhoben wurden.

Auf welchen fachrechtlichen Grundlagen können deutsche Geheimdienste Kommunikationsdaten an ausländische Dienste übermitteln bzw. von diesen entgegennehmen?

Daten aus der strategischen Überwachung des BND dürfen laut Gesetz (§ 7a G10) an ausländische Dienste übermittelt werden, sofern sie zu einem der folgenden drei Gefahrenbereichen erhoben wurden: Terrorismus, Proliferation oder Schleusung. Die Übermittlungsbefugnis bezieht sich nicht auf den gesamten Rohdatenstrom, den der BND für die strategische Überwachung auswertet, sondern allenfalls auf einzelne Kommunikationsvorgänge, die den Suchbegriffen entsprechen, denn § 6 Abs. 1 G10 setzt eine vorherige Prüfung der Relevanz der Daten für den/die Empfänger_in voraus. „Werden diese Kollektivgüter restriktiv bestimmt, so beschränkt sich die Übermittlungsermächtigung auf schwerwiegende Krisenlagen." (Bäcker, S. 15) Die Übermittlung ist nur zulässig, wenn folgende Voraussetzungen erfüllt werden: sie muss zur Wahrung außen- oder sicherheitspolitischer Belange der BRD oder erheblicher Sicherheitsinteressen des Empfängerstaates notwendig sein; es dürfen keine überwiegenden schutzwürdigen Interessen des/der Betroffenen entgegenstehen; im Empfängerstaat muss ein datenschutzkonformer Umgang gewährleistet werden; das Prinzip der Gegenseitigkeit wird gewahrt (d.h. der BND erhält auch Daten der Gegenseite); das Bundeskanzleramt muss der Übermittlung zustimmen. Die Befugnis wird den Berichten des PKGr zufolge entsprechend selten angewandt.

Weitere gesetzliche Bestimmungen zur Übermittlung von TK-Überwachungsdaten an ausländische Stellen finden sich nicht. Das will aber nichts heißen, denn: Zum einen hat die Bundesregierung eingeräumt, dass **Daten aus gezielten geheimdienstlichen Überwachungsmaßnahmen** unter Berufung auf § 4 Abs. 4 G 10-Gesetz übermittelt (werden sollen).(16) Nach dieser Vorschrift – die eigentlich die Weitergabe an deutsche Stellen regelt – dürfen Verkehrs- und Inhaltsdaten zur „Verhinderung oder Aufklärung von Straftaten" eines im Gesetz benannten Straftatenkatalogs übermittelt werden, „soweit sie zur Erfüllung der Aufgaben des Empfängers erforderlich sind." (§ 4 Abs. 4 G 10) Bäcker weist darauf hin, dass dies keine Befugnis für die Übermittlung an ausländische Stellen sei, denn: „Ausländische Stellen sind nicht dazu berufen, Straftaten nach dem StGB zu verhindern oder zu verfolgen, sondern wahren das Strafrecht ihrer Heimatrechtsordnung, das in § 4 Abs. 4 G 10 nicht in Bezug genommen wird. Es entspricht daher auch datenschutzrechtlichen Gepflogenheiten, Datenübermittlungen ins Ausland gesondert und ausdrücklich zu regeln." (Bäcker, S. 7)

Zum anderen ist fraglich, inwiefern amerikanische oder britische Geheimdienste von den offenbar noch

bestehenden **Alliierten-Rechten** Gebrauch machen, wonach sie an TK-Überwachungsmaßnahmen deutscher Behörden teilnehmen (und von deren Ergebnissen profitieren) dürfen (siehe dazu den Beitrag von Deiseroth in diesem Heft).

Für die geheimdienstliche Praxis dürfte schließlich auch entscheidend sein, dass zwischen den Diensten meist keine Rohdaten einer Telefonüberwachung, sondern höchstens die daraus gewonnenen **Erkenntnisse** ausgetauscht werden. Die gesetzlichen Bestimmungen lassen dabei offen, ob für solche Erkenntnisse die restriktiven Übermittlungsvorschriften aus § 7a G 10-Gesetz oder die viel weiter gefassten allgemeinen Vorschriften zur Übermittlung personenbezogener Daten an ausländische Stellen17 anzuwenden sind. Immerhin scheint sich die Bundesregierung an der enger gefassten Auslegung der Norm zu orientieren.(18)

Dennoch bleibt als Ergebnis: Für die Weitergabe von TK-Überwachungsdaten durch den BND bzw. das Bundesamt für Verfassungsschutz existieren nur sehr **spärliche Rechtsgrundlagen und ein großer Graubereich.** Dafür, unter welchen Bedingungen die deutschen Dienste Daten von ihren Partnern annehmen dürfen, finden sich gleich gar keine Regelungen. Dies ist aus verfassungsrechtlicher Sicht umso problematischer, denn die Annahme solcher Daten aus dem Ausland kommt aus grundrechtlicher Sicht einer Befugnis zur Erhebung durch die deutschen Dienste gleich: „Entsprechen die ersten Zugriffe auf die durch Art. 10 GG geschützten Fernmeldevorgänge und Telekommunikationsinhalte seitens der ausländischen Stellen nicht den Anforderungen, die Art. 10 GG an Einschränkungen des Telekommunikationsgeheimnisses stellt, so haftet dieser Makel auch den nachfolgenden Informations- und Datenverarbeitungsprozessen an. Erfolgen diese durch grundrechtsgebundene Träger deutscher öffentlicher Gewalt, so handeln diese Träger grundrechtswidrig.“ (Papier, S. 8)

Die zahlreichen Rechtslücken und Graubereiche des geheimdienstlichen Datenaustauschs spiegeln sich auch in den **Berichtspflichten nach dem G 10-Gesetz** wieder: In den jährlichen Berichten des Kontrollgremiums finden sich keinerlei Angaben zur Übermittlung von Verkehrs- oder Inhaltsdaten aus der gezielten geheimdienstlichen Überwachung. Und für die Annahme sensibler, kommunikationsbezogener Daten von ausländischen Stellen gibt es ebenfalls keine Berichtspflicht – obwohl das Prinzip der Gegenseitigkeit im geheimdienstlichen Datenaustausch ausdrücklich im Gesetz festgeschrieben ist und die Annahme von Daten grundrechtlich nicht weniger problematisch ist als deren Abgabe.

Schutzpflichten des deutschen Staates

Ein weiterer Schwerpunkt der Sachverständigengutachten von Hoffmann-Riem und Papier bilden die sogenannten Schutzpflichten. Die Schutzpflichten sollen – vereinfacht gesagt – die grundrechtlich verbürgten Freiheitsgarantien für die Bürger_innen gewährleisten, indem der Staat entsprechende Vorkehrungen zur Vermeidung bzw. Minderung drohender Grundrechtseinschränkungen trifft. Aus den Schutzpflichten heraus lässt sich die Frage beantworten: Was müssen, sollten oder können die Bundesregierung und die zuständigen Stellen tun, um die Massenüberwachung deutscher Telekommunikation durch ausländische Geheimdienste zu vermeiden?

Für die infrage stehenden Überwachungsvorgänge der NSA und anderer Geheimdienste kommen verschiedene Schutzpflichten in Betracht: das Fernmeldegeheimnis (Art. 10 GG), das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht)(19), der Schutz des Kernbereichs privater Lebensgestaltung (Art. 1 Abs. 1 GG). Für die Wahrnehmung der Schutzaufträge räumt das Verfassungsrecht dem Gesetzgeber einen weitgehenden Handlungsspielraum ein: Er kann nicht auf bestimmte zu ergreifende Maßnahmen verpflichtet werden; dem Rechtsschutz unterliegen die Schutzaufträge nur, sofern der Staat überhaupt keine oder völlig inadäquate Maßnahmen ergreift (vgl.

Papier, S. 10).

Welche Schutzmaßnahmen sind nun aus Sicht der Gutachter geboten? Zuallererst sind die zuständigen Stellen (insbesondere die Strafverfolgungsbehörden und der Verfassungsschutz) dazu verpflichtet, gegen Überwachungsaktivitäten ausländischer Geheimdienste auf deutschem Boden konsequent vorzugehen und diese zu unterbinden. Es gehöre zur „Wahrnehmung staatlicher Schutzaufgaben, die im nationalen Sicherheits- und Ordnungsrecht bestehenden **Befugnisse zur Gefahrenabwehr/-vorsorge** auch zugunsten der Bürger einzusetzen, die von Spähmaßnahmen betroffen sind oder sein können.“ (Hoffmann-Riem, S. 27). Die Einleitung entsprechender Ermittlungsverfahren durch die Strafverfolgungsbehörden sei nach den bisher bekannten Details der Ausspähung von Kommunikationsvorgängen unumgänglich, der Ermessensspielraum für ein strafprozessual begründetes Absehen von der Strafverfolgung deutlich eingeengt (ebd.). Andernfalls mache sich der deutsche Staat mitschuldig an den ausländischen Eingriffen in das Fernmeldegeheimnis, denn: „Eingriffe ausländischer Stellen, die von deutschem Boden aus vorgenommen werden und die mit Billigung oder Duldung deutscher Stellen erfolgen, sind auch der deutschen öffentlichen Gewalt zuzurechnen.“ (Papier, S. 7)

Die Telekommunikationsanbieter seien zu einer deutlichen **Verbesserung der technischen Sicherheitsstandards** ihrer TK-Systeme anzuhalten. Die globale geheimdienstliche Überwachung übersteige bei weitem das Maß der Gefährdungen, die der Entscheidung des Bundesverfassungsgerichts zur sog. Online-Durchsuchung von Computern zugrunde lag, in der das IT-Grundrecht formuliert wurde (Hoffmann- Riem, S. 16). „Es muss daher auf eine Ausgestaltung der informationstechnischen Systeme derart hingewirkt werden, dass sie Sicherheitsanforderungen genügen, die einen Schutz personenbezogener Kommunikation losgelöst von der Möglichkeit der Kenntnisnahme von Eingriffen durch den Betroffenen und damit der individuellen Abwehr gewähren.“ (ebd.) Das heißt in der Praxis: Kommunikationssysteme sind so zu gestalten, dass ihre Benutzer_innen darauf vertrauen können, dass ihre Nachrichten nicht von Dritten unbefugt mitgelesen bzw. erfasst werden. Dem/der Einzelnen ist nicht zuzumuten, dass er/sie sich selbst davon überzeugt, dass ein solches System integer ist (nicht infiltriert wurde) – was bei den heutigen komplexen Netzwerken kaum zu bewerkstelligen ist.

Von der Bundesregierung sei darüber hinaus ein „energischer Einsatz“ für **bilaterale und unilaterale Datenschutzabkommen** zu erwarten, denn letztlich kann ein übergreifender Schutz der globalen Kommunikationsvorgänge nur länderübergreifend funktionieren. (Papier, S. 11) Die dafür möglichen Instrumente sind bekannt: EU-Datenschutzgrundverordnung(20), die Aussetzung bzw. Neuverhandlung des Safe Harbor-Abkommens und der Vereinbarungen zu SWIFT und PNR(21), eine internationale Konvention zum Datenschutz.(22)

Eine weitere Empfehlung an den Gesetzgeber ist die **Verschärfung der strafrechtlichen Normen** gegen das unbefugte Ausspähen und Abfangen von Daten (§§ 202 a und b StGB) sowie die Umstellung für diese Delikte vom Tatort- auf das Schutzprinzip (analog zu den §§ 5 und 6 StGB). Damit würden auch Abhörmaßnahmen gegen deutsche Telekommunikationsvorgänge im Ausland hierzulande verfolgbar, die Strafnormen dem extraterritorialen Charakter des Grundrechts angeglichen (Papier, S. 10f.).

Daran anschließend ließe sich auch fragen, ob es nach der NSA-Affäre noch zeitgemäß ist, dass sich das strafrechtliche Verbot der Verletzung des Post- oder Fernmeldegeheimnisses (§ 206 StGB) bislang nur auf einen sehr beschränkten Personenkreis erstreckt.Die Strafnorm gilt nur für Beschäftige und Auftragnehmer_innen von TK-Firmen und Dienstleistern, für Personen, die Aufsichtsfunktionen gegenüber oder sonstige Arbeiten in TK-Unternehmen wahrnehmen sowie für Amtsträger_innen. Für andere (etwa die Mitarbeiter_innen ausländischer Geheimdienste), die sich von außen, auch ohne Mitwirkung der Betreiber_innen Zugang zu Telekommunikationseinrichtungen verschaffen, kommt nur der allgemeinere Tatbestand des Ausspähens und Abfangens von Daten (s.o.) in Betracht.

Hoffmann-Riem ruft den Gesetzgeber darüber hinaus auch zu einer **Weiterentwicklung geltender Rechtsgrundlagen** auf, um den gesteigerten Gefährdungen der Kommunikationsgrundrechte zu begegnen. Als erstes benennt er dabei die Gewährleistung eines flächendeckenden und angemessenen Angebots an

Telekommunikationsdienstleistungen, die in Artikel 87f Abs. 1 GG festgehalten ist. Diese Norm soll bisher sicherstellen, dass ein hinreichend dichtes und qualitativ angemessenes Angebot an TK-Dienstleistungen verfügbar ist. Dazu zähle heute auch die Gewissheit, dass die Kommunikation vertraulich und das TK-System nicht kompromittiert sei: „Angemessen ist eine Kommunikationsversorgung nur, wenn sie auch Schutz vor Ausspähung, Manipulation und sonstigen Beeinträchtigungen freier Kommunikation gewährt. Der Maßstab der Angemessenheit kann in systematischer Interpretation auch unter Rückgriff auf die Garantien der Kommunikationsgrundrechte … inhaltlich aufgefüllt und gegebenenfalls im Zuge einer Rechtsfortbildung auf neue Lagen erstreckt werden.“ (Hoffmann-Riem, S. 17)

Ein weiterer Schutzanspruch ließe sich nach Hoffmann-Riem aus Artikel 91c GG ableiten. Diese Norm regelt die Zusammenarbeit von Bund und Ländern bei Planung, Einrichtung und Betrieb von gemeinsam genutzten informationstechnischen Systemen. Sie soll gewährleisten, dass die Zusammenarbeit nicht an inkompatiblen Systemen scheitert und die öffentlichen IT-Infrastrukturen ein ausreichendes Sicherheitsniveau aufweisen. Da Bund und Länder in vielen Bereichen auf die allgemeine Infrastruktur des Internets zurückgreifen, „erstreckt die Aufgabe sich [auch] auf die Nutzung der allgemein nutzbaren Netze. Dies betrifft auch die Kommunikation mit den Bürgern, etwa im Rahmen des E-Government. Insofern müssen sich Sicherheitsanforderungen auch auf Kommunikation außerhalb des internen Behördenbetriebs beziehen.“ (Hoffmann-Riem, S. 18) Weitere Vorschläge zur Rechtsentwicklung beziehen sich auf völkerrechtliche Anknüpfungspunkte.

Neben den Schutzpflichten bietet auch der abwehrende **grundrechtliche Schutzbereich des Fernmeldegeheimnisses,** den das Bundesverfassungsgericht durch seine Rechtsprechung maßgeblich gestaltet hat, Raum für Verbesserungen. So bezieht sich das Fernmeldegeheimnis zwar auf die Inhalte und Umstände der Kommunikation sowie aller Kommunikationsversuche, jedoch hat es das Gericht bisher abgelehnt, auch die von den Telekommunikationsgeräten erzeugten Steuersignale (z.B. das Einbuchen von Handys in Mobilfunkzellen) dem grundrechtlichen Schutz zu unterstellen.23 Diesem Datenaustausch kann sich jedoch kein_e Handynutzer_in entziehen, außer sie/er schaltet das Gerät ab. Mit dieser Rechtsprechung ebnete das Gericht einer massenhaften Identifizierung und Ortung von Handys durch IMSI-Catcher und stille SMS den Weg.

Unter dem Gesichtspunkt der sich wandelnden Kommunikationsgewohnheiten könnte man ebenso fragen, ob die verfassungsrechtliche Beschränkung des Fernmeldegeheimnisses auf laufende Kommunikationsvorgänge nicht überholt ist. Sie hat zur Folge, dass der grundrechtliche Schutz nach dem Ende des Gesprächs bzw. der ersten Kenntnisnahme einer Nachricht (z.B. E-Mail) endet. Das mag bei Telefonaten seinen Sinn haben. Im Zeitalter der E-Mail-Kommunikation, bei der die meisten Nachrichten standardmäßig auch nach dem Lesen auf den Mailservern der Empfänger_innen gespeichert bleiben, entstehen dadurch große Datensammlungen, die vergleichsweise schwachen Grundrechtsschutz genießen.

Zur Frage des Schutzbereichs gehört auch, dass der oben angesprochene extraterritoriale Geltungsbereich des Grundrechts (den das Gericht anerkennt) schon aus Gründen der Klarheit und Rechtssicherheit in der Verfassung explizit gemacht werden sollte.

Rechtspolitisch bleibt also viel zu tun.

SVEN LÜDERS Jahrgang 1973, ist gelernter Soziologe und seit 2004 Geschäftsführer der Humanistischen Union.

Anmerkungen:

(1) Die Stellungnahmen der Gutachter – die nachfolgend nur verkürzt zitiert werden – sind auf der Webseite

des Deutschen Bundestags abrufbar unter
http://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848.

(2) BVerfG, Urteil vom 2.3.2010, 1 BvR 256/08 (=BVerfGE 125, 260).

(3) Außen vor bleibt im Bäcker-Gutachten eine weitere Rechtsgrundlage für die strategische Fernmeldeaufklärung durch den BND nach § 8 G10, die jedoch auf eng umgrenzte Gefahrensituationen für Leib und Leben einer Person beschränkt ist und deshalb praktisch nur bei Entführungsfällen deutscher Staatsbürger_innen im Ausland anzuwenden wäre. Vgl. dazu den Aufsatz von Huber in diesem Heft, Abschnitt IIIc.

(4) Nach dem oben zitierten Urteil des BVerfG dürfen solche Verkehrsdaten von den Diensteanbietern nur gespeichert werden, sofern sie für Abrechnungszwecke oder aus Gründen der technischen Absicherung der Dienste notwendig sind. In der Praxis speichern viele Anbieter die Verkehrsdaten 14 Tage lang.

(5) Bäcker verweist auf ein weiteres Problem der gezielten TK-Überwachung: Einmal von den Geheimdiensten erhobene / erworbene Daten müssen nach § 4 Abs. 1 G10-Gesetz unverzüglich nach der Erhebung, und dann regelmäßig alle sechs Monate auf ihre nachrichtendienstliche Relevanz geprüft werden und sind – sofern sie nicht mehr zur Aufgabenerfüllung oder für die Übermittlung an Dritte benötigt werden – zu löschen. Das klingt nach Datensparsamkeit, ist aber das genaue Gegenteil. Die für die Speicherung genannten Aufgaben, an denen sich die Löschung orientiert, sind nämlich erheblich weiter gefasst als jene Anlässe, unter denen die Daten erhoben wurden. Beim Übergang von der Erhebung zur Speicherung von Daten aus der Fernmeldeüberwachung findet also in Art. 4 Abs. 1 G10 eine erhebliche Zweckerweiterung statt. „Einmal erlangte Daten dürfen also nahezu umfassend bevorratet, ausgewertet und genutzt werden, soweit aus ihnen überhaupt Informationen gewonnen werden können, die für den erhebenden Nachrichtendienst relevant sind.“ (Bäcker, S. 6f.)

(6) Zum Vorgehen des BND sowie dem Genehmigungs- und Kontrollverfahren vgl. den Beitrag von Huber in diesem Heft.

(7) BVerfG, Urteil des Ersten Senats vom 14.07.1999 - 1 BvR 2226/94 u.a.

(8) S. Parlamentarisches Kontrollgremium (PKGr): Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) ..., BT-Drs. 17/12773 v. 14.3.2013, S. 7.

(9) S. BVerwG, Urteil v. 28.5.2014 – 6 A 1.13; Christian Rath, Verfassungsbeschwerde zurückgezogen – BND muss sich nicht sorgen, tageszeitung v. 21.10.2014.

(10) B. Huber: Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite. NJW 35/2013, S. 2572-2577; vgl. auch den Beitrag von Huber in diesem Heft.

(11) Ebd., S. 2575.

(12) Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion Bündnis 90/Die Grünen, BT-Drs. 17/14739 v. 12.09.2013 sowie Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD, BT-Drs. 17/14560 v. 14.08.2013.

(3)Die zitierten Normen lauten: „Der Bundesnachrichtendienst sammelt zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus. Werden dafür im Geltungsbereich dieses Gesetzes Informationen einschließlich personenbezogener Daten erhoben, so richtet sich ihre Erhebung, Verarbeitung und Nutzung nach den §§ 2 bis 6 und 8 bis 11.“ (§ 1 Abs. 2 BNDG) sowie „Der Bundesnachrichtendienst darf die erforderlichen Informationen einschließlich personenbezogener Daten erheben, verarbeiten und

nutzen, soweit nicht die anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes oder besondere Regelungen in diesem Gesetz entgegenstehen, ... über Vorgänge im Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, wenn sie nur auf diese Weise zu erlangen sind und für ihre Erhebung keine andere Behörde zuständig ist.“ (§ 2 Abs. 1 Nr. 4 BNDG)

(14) S. Stefan Heumann/Ben Scott: Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany. Impulse 25/13, Berlin 2013.

(15) Bäcker (S. 15) weist darauf hin, dass diese Ungleichbehandlung verfassungswidrig ist, da das Fernmeldegeheimnis unterschiedslos für In- und Ausländer_innen gilt. Die unterschiedlichen Eingriffsschwellen für die Überwachung (etwa bei der strategischen Fernmeldeaufklärung) verstoßen deshalb gegen den Gleichheitsgrundsatz aus Artikel 3 Abs. 1 GG.

(16) S. Antwort der Bundesregierung auf eine Kleine Anfrage der SPD-Fraktion, BT-Drs. 17/14560 v. 14.08.2013, S. 24.

(17) Die Übermittlung solcher Informationen – ohne Bezug zur Telekommunikation – richtet sich nach § 19 Abs. 2 und 3 BVerfSchG i.V.m. § 9 Abs. 2 BNDG. Die Übermittlung ist demnach einerseits an Dienststellen der amerikanischen Stationierungsstreitkräfte in Deutschland zulässig, sofern die deutschen Behörden dazu im Rahmen der Zusatzvereinbarung zum NATO-Truppenstatut verpflichtet sind (d.h sofern es ein entsprechendes Begehren von dieser Seite gibt). Für alle anderen Übermittlungen an ausländische Stellen gilt: Sie ist für den BND nur zulässig, sofern „sie zur Wahrung außen- und sicherheitspolitischer Belange der Bundesrepublik Deutschland erforderlich ist und das Bundeskanzleramt seine Zustimmung erteilt hat“ (§ 9 Abs. 2 BNDG). Hoffmann-Riem weist darauf hin, dass diese Übermittlungsbefugnis keine Weitergabe von Rohdaten gestattet, da „die tatbestandlichen Voraussetzungen der Datenübermittlung noch gar nicht festgestellt worden“ sind (Hoffmann-Riem, S. 12).

(18) Vgl. Bäcker S. 16 und BT-Drs. 17/14560 (s. Anm. 16).

(19) BVerfG, Urteils v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 („Online-Durchsuchung“).

(20) S. die Beiträge von Deiseroth (Thesen 5 und 6) sowie Dix in diesem Heft.

(21) S. den Beitrag von Dix in diesem Heft.

(22) S. den Beitrag von Töpfer in diesem Heft.

(23) BVerfG, Urteil v. 22.8.2006 – 2 BvR 1345/03. Das Gericht sah in dem ständigen Datenaustausch zwischen eingeschaltetem Handy und Funknetz keinen Bezug zu einer laufenden Kommunikation; der Vorgang diene lediglich der Herstellung der Kommunikationsbereitschaft und unterliege deshalb nicht dem Schutzbereich von Art. 10 GG. Ausführlicher zu der Entscheidung über eine Musterklage der Humanistischen Union s. Rosemarie Will, Kein Grundrechtsschutz für Handybenutzer?, in: Gustav Heinemann-Initiative/Humanistische Union (Hrsg.), Graubuch Innere Sicherheit. Berlin 2009, S. 100 ff.
