Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)653 E

Deutsches Institut
für Menschenrechte

Stellungnahme

# Menschenrechtliche Anforderungen an die Ausland-Ausland-Fernmeldeaufklärung und ihre Kontrolle

Öffentliche Anhörung des Innenausschusses des Deutschen Bundestages am 26. September 2016

**September 2016**

## Inhalt

# 1 Vorbemerkung

Unter dem Eindruck der Enthüllungen Edward Snowdens über das Ausmaß der globalen nachrichtendienstlichen Kommunikationsüberwachung und maßgeblich vorangetrieben durch die Bundesregierung verabschiedete die Generalversammlung der Vereinten Nationen am 18. Dezember 2013 die Resolution 68/167 zum „Recht auf Privatsphäre im digitalen Zeitalter“. Darin zeigt sich Generalversammlung „tief besorgt über die nachteiligen Auswirkungen, die das Überwachen und/oder Abfangen von Kommunikation, einschließlich des extraterritorialen Überwachens und/oder Abfangens von Kommunikation, sowie die Sammlung personenbezogener Daten, insbesondere wenn sie in massivem Umfang durchgeführt werden, auf die Ausübung und den Genuss der Menschenrechte haben können“. Sie bekräftigt, dass die Menschenrechte und insbesondere das Recht auf Privatsphäre sowohl „offline“ als auch „online“ gleichermaßen gelten. Die Staaten werden aufgefordert, das Recht auf Privatsphäre auch bei digitaler Kommunikation zu achten und zu schützen, Maßnahmen zu ergreifen, um Rechtsverletzungen zu beenden und zukünftig zu verhindern, nationales Recht und Praktiken der Kommunikationsüberwachung zu überprüfen und in Einklang mit internationalen Menschenrechtsverpflichtungen zu bringen sowie eine unabhängige und effektive Aufsicht zu gewährleisten.[1]

Entsprechend ist es uneingeschränkt zu begrüßen, dass in Deutschland mit dem 1. Untersuchungsausschuss des 18. Deutschen Bundestages weltweit einer der wenigen Versuche einer intensiven parlamentarischen Aufarbeitung der rechtlichen, technischen und politischen Fragen rund um die Kommunikationsüberwachung der „Five Eyes“ und der Beteiligung deutscher Behörden unternommen wird und mit den nun vorliegenden Vorschlägen für Reformen erste Lehren aus den Untersuchungsergebnissen gezogen werden sollen.

Mit den vorliegenden Reformvorschlägen zielen zum einen die Fraktionen von CDU/CSU und SPD darauf, die auf außerdeutsche Kommunikationsbeziehungen gerichteten SIGINT-Aktivitäten des Bundesnachrichtendienstes (BND) gesetzlich zu regeln (BT-Drs. 18/9041). Zum anderen wollen sowohl die Koalition als auch die Opposition die Kontrolle der Nachrichtendienste des Bundes u.a. durch Änderungen des Kontrollgremiumgesetzes (PKGrG) verbessern (BT-Drs. 18/9040, 18/6640, 18/6645, 18/8163). Dabei weisen die Vorschläge zum Beispiel beim Whistleblower-Schutz in eine identische Richtung, unterscheiden sich aber deutlich, etwa wenn es um die Minderheitenrechte im Kontrollgremium oder um die Zukunft des Vertrauensgremiums und der G 10-Kommission geht.

Die vorliegende Stellungnahme kommentiert die Vorschläge aus einer menschenrechtlichen Perspektive. Damit will sie einen Beitrag dazu zu leisten, dass die Bundesrepublik das Recht der nachrichtendienstlichen Fernmeldeaufklärung und ihrer Kontrolle in Überstimmung mit den völkerrechtlichen Vorgaben insbesondere aus dem Internationalen Pakt über bürgerliche und politische Rechte (IPbpR - Zivilpakt) sowie der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) bringt und auf diesem Wege ihre positive Rolle beim globalen

---

[1] UN, General Assembly (2013): The right to privacy in the digital age. Resolution. UN Dok. A/RES/68/167 vom 18.12.2013. Deutsche Übersetzung unter: http://menschenrechte-durchsetzen.dgvn.de/fileadmin/user_upload/menschenr_durchsetzen/bilder/News/Menschenrechte_im_digitalen_Zeitalter/GV_Resolution_68_167_Menschenrechete_im_dig._Zeitalter_2013-ar68167.pdf

Schutz des Menschenrechts auf Privatsphäre fortführt und ein Beispiel für andere Staaten setzt.

Unstrittig ist, dass die Ausübung des Rechts auf Privatsphäre auch für die Verwirklichung anderer Menschenrechte wichtig ist: Wer fürchtet, dass seine Kommunikation überwacht wird, fürchtet vielleicht auch, seine Meinung offen zu äußern, freien Zugang zu Informationen zu suchen, eine politische Versammlung zu besuchen, ärztlichen, anwaltlichen oder seelsorgerischen Rat einzuholen oder sich an Vertreter der Presse zu wenden, um auf Missstände aufmerksam zu machen. Ist das Menschenrecht auf Privatsphäre in Gefahr, können auch das Recht auf Meinungs- und Informationsfreiheit, das Recht auf Versammlungs- und Vereinigungsfreiheit, das Recht auf Gesundheit, das Recht auf Religionsfreiheit und das Recht auf ein faires Verfahren bedroht sein. Wichtig ist es daher, die Reformpläne auch aus dieser Perspektive zu hinterfragen und zum Beispiel Garantien für den Schutz privilegierter Kommunikation zu diskutieren.[2] Die vorliegende Stellungnahme beschränkt sich jedoch aus Zeitgründen auf die menschenrechtlichen Anforderungen, die sich aus dem Recht auf Privatsphäre an die Ausgestaltung nachrichtendienstlicher Kommunikationsüberwachung und ihrer Kontrolle ergeben.

# 2 Das Menschenrecht auf Privatsphäre

## 2.1 Schutz- und Geltungsbereich

Das Menschenrecht auf Privatsphäre schützt nach Art. 17 Zivilpakt und Art. 8 EMKR die „Korrespondenz“ aller Personen im Anwendungsbereich der Menschenrechtsverträge vor willkürlichen und rechtswidrigen Eingriffen. Sowohl der UN-Menschenrechtsausschuss als auch der Europäische Gerichtshof für Menschenrechte (EGMR) haben klargestellt, dass der Begriff der „Korrespondenz“ zeitgemäß auszulegen ist und auch elektronische Kommunikation wie Telefonate, Fax oder Emails vom Schutzbereich umfasst sind.[3] Konsequenterweise schützen Menschenrechtsverträge jüngeren Datums wie zum Beispiel die UN-Behindertenrechtskonvention ausdrücklich auch „andere Arten der Kommunikation“ (Art. 22 UN-BRK). Konsens besteht mittlerweile auch darüber, dass der Schutz nicht nur für Kommunikationsinhalte, sondern auch für Standort-, Verbindungs- und andere sogenannte Metadaten gilt, da deren Aggregation die Erstellung detaillierter Persönlichkeitsprofile ermöglicht.[4]

---

2 Siehe das Schreiben der drei UN-Sonderberichterstatter David Kaye (Mandat zum Recht auf Meinungsfreiheit), Michel Forst (Mandat zur Situation von Menschenrechtsverteidiger) und Mónica Pinto (Mandat zur Unabhängigkeit von Richtern und Anwälten) vom 29.08.2016 mit Fragen zur geplanten Reform an den deutschen Botschafter bei den Vereinten Nationen: http://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_DEU_2.2016.pdf. Vgl. auch Venice Commission (2015): Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies. CDL-AD(2015)006. Strasbourg (Study; 719/2013), 07.04.2015, Rn. 106ff.

3 UN, Human Rights Committee (1988): CCPR General Comment No. 16. Article 17 (Right to privacy). UN Dok. CCPR/GEC/6624 vom 08.04.1988, Rn. 8; EGMR (1978): Klass und andere gegen Deutschland. Urteil vom 06.09.1978. Beschwerdenr. 5029/71, Rn. 41; EGMR (2008): Liberty und andere gegen das Vereinigte Königreich. Urteil vom 01.07.2008. Beschwerdenr. 58243/00, Rn. 56. Siehe auch Schiedermair, Stephanie (2012): Der Schutz des Privaten als internationales Grundrecht. Tübingen: Mohr Siebeck, S. 219ff.

4 EGMR (1984): Malone gegen das Vereinigte Königreich. Urteil vom 02.08.1984. Beschwerdenr. 8691/79, Rn. 84; UN, Human Rights Council (2013): Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. UN Dok. A/HRC/23/40 vom 17.04.2013, Rn. 15; Ders. (2014): The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. UN Dok. A/HRC/27/37 vom 30.06.2014, Rn. 19; UN, General Assembly (2014): Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. UN Dok. A/69/397 vom 23.09.2014. Rn. 53. UN, General Assembly (2014): The right to privacy in the digital age. Resolution. UN Dok. A/RES/69/166 vom 18.12.2014.

Geschützt ist nicht nur die Kommunikation von Personen, die sich auf dem Territorium einer Partei der internationalen Menschenrechtsverträge befinden, sondern auch jene von Kommunikationsteilnehmern im Ausland. Entscheidend ist die stabile Kontrolle einer Vertragspartei über die genutzte Kommunikationsinfrastruktur. Hierzu schreibt das UN-Hochkommissariat für Menschenrechte:

> „In Artikel 2 des Internationalen Paktes über bürgerliche und politische Rechte wird jeder Vertragsstaat dazu verpflichtet, die in dem Pakt anerkannten Rechte zu achten und sie allen in seinem Gebiet befindlichen und seiner Herrschaftsgewalt unterstehenden Personen ohne Unterschied […] zu gewährleisten. Der Menschenrechtsausschuss erklärte in seiner Allgemeinen Bemerkung Nr. 31, dass in Artikel 2 Absatz 1 ‚von den Vertragsstaaten verlangt wird, die Paktrechte zu achten und sie allen in ihrem Gebiet befindlichen und ihrer Herrschaftsgewalt unterstehenden Personen zu gewährleisten. Dies bedeutet, dass ein Vertragsstaat die im Pakt niedergelegten Rechte achten und sie jeder Person, die seiner Gewalt oder tatsächlichen Kontrolle unterliegt, gewährleisten muss, auch wenn sie sich nicht im Gebiet des Vertragsstaats befindet.‘ […] Der Menschenrechtsausschuss hat sich von dem schon in seinen frühesten Entscheidungen geäußerten Grundsatz leiten lassen, dass ein Staat sich seinen Verpflichtungen auf dem Gebiet der internationalen Menschenrechte nicht entziehen kann, indem er außerhalb seines Hoheitsgebiets Maßnahmen vornimmt, die ihm „im eigenen Land“ untersagt wären. […] Die Begriffe ‚Gewalt‘ und ‚tatsächliche Kontrolle‘ sind Indikatoren dafür, ob ein Staat ‚Herrschaftsgewalt‘ oder hoheitliche Befugnisse ausübt, deren Missbrauch durch Vorschriften zum Schutz der Menschenrechte eingeschränkt werden soll. Ein Staat kann sich seinen menschenrechtlichen Verantwortlichkeiten nicht einfach dadurch entziehen, dass er es unterlässt, Befugnisse dieser Art rechtlich einzugrenzen. Ein anderer Schluss würde nicht nur die Universalität und den Wesensgehalt der durch die internationalen Menschenrechtsnormen geschützten Rechte untergraben, sondern möglicherweise auch strukturelle Anreize für Staaten schaffen, Überwachungsaktivitäten wechselseitig auszulagern. Daraus folgt, dass digitale Überwachungsmaßnahmen die Menschenrechtsverpflichtungen eines Staates berühren können, wenn die Überwachung mit der Ausübung staatlicher Gewalt oder tatsächlicher Kontrolle in Bezug auf digitale Kommunikationsinfrastruktur, gleich wo sich diese befindet, durch den Staat verbunden ist, beispielsweise durch direktes Abhören oder durch Eindringen in diese Infrastruktur.“[5]

Entsprechend betonte auch der UN-Menschenrechtsausschuss zum Abschluss der jüngsten Staatenberichtsverfahren gegenüber drei der „Five Eyes“ (USA, Vereinigtes Königreich und Neuseeland) ausdrücklich, dass bei Eingriffen in das Recht auf Privatsphäre menschenrechtliche Standards zu beachten sind „unabhängig von der Nationalität oder dem Ort der betroffenen Individuen“.[6]

---

5 UN, Human Rights Council (2014): The right to privacy in the digital age. Report. UN Dok A/HRC/27/37 vom 30.06.2014, Rn. 32f.

6 UN, Human Rights Committee (2014): Concluding observations on the fourth periodic report of the United States of America. UN Dok. CCPR/C/USA/CO/4 vom 26.03.2014, Rn. 22; Ders. (2015): Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland. UN Dok. CCPR/C/GBR/CO/7 vom 21.07.2015, Rn. 24; Ders. (2016): Concluding observations on the sixth periodic report of New Zealand. UN Dok. CCPR/C/NZL/CO/6 vom 24.03.2016, Rn. 16.

Dass stabile Kontrolle bzw. „Hoheitsgewalt“ i.S.v. Art. 1 EMRK nicht nur im Inland ausgeübt wird, sondern auch in Räumen außerhalb des Staatsgebietes einer Vertragspartei wie etwa militärisch besetzten Gebieten, diplomatischen Vertretungen, Flugzeugen oder Schiffen auf Hoher See, hat auch der Europäische Gerichtshof für Menschenrechte (EGMR) in verschiedenen Entscheidungen deutlich gemacht.[7] Mindestens für solche Exklaven extraterritorialer Herrschaft ist nach dessen Rechtsprechung daher davon auszugehen, dass die menschenrechtlichen Verpflichtungen auch zur Achtung des Rechts auf Privatsphäre gelten. Überdies wurde im Fall Liberty u.a. gegen das Vereinigte Königreich weder vom EGMR noch von der britischen Regierung bestritten, dass zwei Beschwerde führende irische Organisationen durch die weitreichenden Befugnisse britischer Nachrichtendienste zur Kommunikationsüberwachung in ihren Rechten verletzt worden waren, obwohl sie ihren Sitz in Dublin – außerhalb britischen Hoheitsgebietes – haben.[8]

## 2.2 Eingriffsvoraussetzungen

Dabei ist das Menschenrecht auf Privatsphäre keineswegs absolut. Immer dann und überall dort, wo Eingriffe in das Menschenrecht auf Privatsphäre und vertrauliche Kommunikation stattfinden, müssen diese einen legitimen Zweck verfolgen, rechtmäßig und notwendig sein. Nach Art. 8 Abs. 2 EGMR ist ein Eingriff nur dann erlaubt, wenn er „gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.“ Art. 17 Zivilpakt listet dagegen keine expliziten Grenzen für eine Beschränkung des Rechts auf Privatsphäre auf. Allerdings hat der Menschenrechtsausschuss in seinen Allgemeinen Bemerkungen zu Art. 17 und in Entscheidungen zu Individualbeschwerden deutlich gemacht, dass Eingriffe nur erfolgen dürfen, wenn sie „unverzichtbar im gesellschaftlichen Interesse“ und verhältnismäßig sind.[9]

Der EGMR überlässt die Abwägung, welche Eingriffe gegenüber welchen Bedrohungen notwendig sind, weitgehend den Mitgliedstaaten, denen er im Feld der nationalen Sicherheit einen breiten Beurteilungsspielraum zugesteht.[10] Gleichwohl erteilt der Gerichtshof damit keinen Freibrief für geheime Überwachungsoperationen der Exekutive. Vielmehr stellt er klar, dass ausreichende und wirksame Garantien gegen Willkür existieren müssen, und betont die besonderen Gefahren für eine Demokratie, wenn das Risiko eines systematischen Machtmissbrauchs besteht. Daher müssen Überwachungsmaßnahmen eine gesetzliche Grundlage haben, die die näheren Umstände der Überwachung spezifiziert und öffentlich bekannt macht und

---

7 Vgl. die Zusammenfassung der Rechtsprechung bei Milanovic, Marko (2015): Human rights treaties and foreign surveillance. Privacy in the digital age. In: Harvard International Law Journal 56 (1), S. 81–146 (S. 112ff.). http://www.harvardilj.org/wp-content/uploads/561Milanovic.pdf.

8 EGMR (2008): Liberty und andere gegen das Vereinigte Königreich. Urteil vom 01.07.2008. Beschwerdenr. 58243/00.

9 UN, Human Rights Committee (1988): CCPR General Comment No. 16. Article 17 (Right to privacy). UN Dok. CCPR/GEC/6624 vom 08.04.1988; Ders. (1994): Toonen gegen Australien. UN Dok. CCPR/C/50/D/488/1992 vom 31.03.1994; Ders. (2004): Van Hulst gegen die Niederlande. UN Dok. CCPR/C/82/D/903/1999 vom 01.11.2004, Rn. 7.6.

10 EGMR (2010): Kennedy gegen das Vereinigte Königreich. Urteil vom 18.05.2010. Beschwerdenr. 26839/05, Rn, 151ff.

somit ein Maß an Vorhersehbarkeit garantiert, insbesondere da die verfügbaren Technologien zunehmend komplexer und undurchsichtiger werden.[11]

Darüber hinaus muss die Ermächtigungsgrundlage nach der EGMR-Rechtsprechung in Einklang mit dem Rechtsstaatsprinzip stehen und einen wirksamen Rechtsschutz gegen willkürliche und rechtswidrige Eingriffe garantieren. Da bei heimlichen Maßnahmen, über die Betroffene häufig auch nach ihrer Beendigung keine Kenntnis erhalten, eine anschließende gerichtliche Überprüfung kaum möglich ist, sind ersatzweise Verfahren zu etablieren, die „adäquate und gleichwertige Garantien“ zum Schutz der Betroffenenrechte gewährleisten.[12]

Vergleichbare Prinzipien hat auch der UN-Menschenrechtsausschuss seit den 1990er für die menschenrechtlichen Anforderungen an die heimliche Überwachung elektronischer und digitaler Kommunikation entwickelt.[13] Zusammengefasst hat er sie in den Abschließenden Bemerkungen zu den jüngsten Staatenberichten der USA und des Vereinigten Königreichs zur Umsetzung des Zivilpaktes vom März 2014 bzw. Juli 2015. Demnach sollen die Vertragsparteien sicherstellen, dass jeder Eingriff in das Recht auf Privatsphäre durch Gesetze autorisiert ist, die

> (i) öffentlich zugänglich sind;
> (ii) Vorschriften beinhalten, die gewährleisten, dass die Erhebung von, der Zugriff auf und die Nutzung von Kommunikationsdaten auf bestimmte legitime Zwecke beschränkt sind;
> (iii) hinreichend präzise sind und ausführlich festlegen die genauen Umstände, unter denen solche Eingriffe genehmigt werden können, Genehmigungsverfahren, die Personenkategorien, die überwacht werden können, Fristen für die Dauer der Überwachung, Verfahren für die Nutzung sowie die Speicherung der erhobenen Daten; und
> (iv) wirksame Schutzmechanismen gegen Missbrauch vorsehen.[14]

# 3 Bewertung und Empfehlungen

## 3.1 Auslandsaufklärung menschenrechtlich begrenzen

Mit dem Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs. 18/9041) soll eine spezifische gesetzliche

---

11 EGMR (2006): Weber und Saravia gegen Deutschland. Entscheidung vom 29.06.2006. Beschwerdenr. 54934/00, Rn. 93ff.

12 EGMR (1978): Klass und andere gegen Deutschland, Rn. 55.

13 U.a. UN, Human Rights Committee (1997): Consideration of reports submitted by State Parties under Article 40 of the Covenant. Concluding Observations of the Human Rights Committee - Jamaica. UN Dok. CCPR/C/79/Add.83 vom 24.10.1997, Rn. 20; Ders. (1999): Consideration of reports submitted by State Parties under Article 40 of the Covenant. Concluding Observations of the Human Rights Committee - Poland. UN Dok. CCPR/C/79/Add.110 vom 28.07.1999, Rn. 22; Ders. (2006): Consideration of reports submitted by States parties under article 40 of the Covenant. Concluding observations of the Human Rights Committee - Republic of Korea. UN Dok. CCPR/C/KOR/CO/3 vom 02.11.2006, Rn. 9; Ders. (2009): Consideration of reports submitted by States parties under article 40 of the Covenant. Concluding observations of the Human Rights Committee - Sweden. UN Dok. CCPR/C/SWE/CO/6 vom 02.04.2009, Rn. 18;

14 Übersetzung des Autors. Im Original: „Ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that: (i) are publicly accessible; (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance; procedures for the use and storage of data collected; and (iv) provide for effective safeguards against abuse“. UN, Human Rights Committee (2014): Concluding observations on the fourth periodic report of the United States of America. UN Dok. CCPR/C/USA/CO/4 vom 26.03.2014, Rn. 22; Ders. (2015): Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland. UN Dok. CCPR/C/GBR/CO/7 vom 21.07.2015, Rn. 24.

Grundlage geschaffen werden für die Erhebung von Daten der Telekommunikation zwischen ausländischen Anschlüssen vom Inland aus sowie für die inländische Verarbeitung und Nutzung von ebensolchen Daten, die durch den BND im Ausland erhoben wurden.

Nach § 8 Abs. 1 BNDG-E sollen inländische Telekommunikationsdienstleister künftig durch Anordnungen verpflichtet werden können, Daten aus Telekommunikationsnetzen, über die Kommunikation von Ausländern im Ausland erfolgt, an den BND auszuleiten oder dem Dienst selbst die Überwachung und Aufzeichnung zu ermöglichen. Zuwiderhandlungen gegen Anordnungen sollen nach § 35 BNDG-E mit Geldbußen bis zu 20.000 Euro geahndet werden können. Bei der Ausland-Ausland-Fernmeldeaufklärung vom Inland aus ist deshalb in jedem Fall von einer stabilen Kontrolle deutscher Stellen über die Kommunikationsinfrastruktur und somit bei der Erhebung von Inhalts- und Metadaten von einem Eingriff in das Recht auf Privatsphäre auszugehen, selbst wenn die betroffenen Personen im Ausland leben.

Es ist daher zu begrüßen, dass das Handeln des BND, anders als bisher, auf eine spezifische gesetzliche Grundlage gestellt werden und nicht länger nur aus der allgemeinen Aufgabenbeschreibung in § 1 Abs. 2 BNDG abgeleitet werden soll. Fraglich ist, ob die weiten Eingriffsbefugnisse, die der Gesetzentwurf für die Ausland-Ausland-Fernmeldeaufklärung des BND vorsieht, legitimen Zwecken dienen und den Standards entsprechen, die EGMR und UN-Menschenrechtsausschuss für die Überwachung von Telekommunikation entwickelt haben.

Zweifellos ist es im berechtigten Interesse der Bundesregierung, über gute und valide Erkenntnisse zu Vorgängen von außen- und sicherheitspolitischer Relevanz zu verfügen und so zum Beispiel bei internationalen Krisen wie dem Konflikt zwischen der Ukraine und Russland nicht von der Propaganda der Konfliktparteien abhängig zu sein. Bei der Erhebung von Kommunikationsdaten nach § 6 BNDG-E wird jedoch, anders als beim Abschöpfen von menschlichen Quellen oder einer Satellitenüberwachung, notwendigerweise in das Recht auf Privatsphäre eingegriffen.

Gerechtfertigt sind solche Eingriffe nur im Rahmen der Schranken-Schranken nach Art. 8 Abs. 2 EMRK. Nach § 6 Abs. 1 BNDG-E soll der BND ermächtigt werden, auf Anordnung des Bundeskanzleramtes Daten aus Telekommunikationsnetzen zu erheben nicht nur zur Aufklärung von Gefahren für die innere und äußere Sicherheit, sondern auch zur Wahrung der Handlungsfähigkeit Deutschlands und zur Gewinnung sonstiger Erkenntnisse von außen- und sicherheitspolitischer Bedeutung entsprechend des Auftragsprofils der Bundesregierung. Dabei bleibt unbestimmt, was unter „Handlungsfähigkeit“ oder „sonstigen Erkenntnissen von außen- und sicherheitspolitischer Bedeutung“ zu verstehen ist. Auch die Begründung des Gesetzentwurfs schweigt sich hierzu aus und erläutert nur, dass zur Wahrung der Handlungsfähigkeit auch die „Aufklärung von wirtschaftspolitisch bedeutsamen Vorgängen“ erforderlich sein kann und eine „Erforderlichkeit zur Gewinnung von sonstigen Erkenntnissen von außen- und sicherheitspolitischer Bedeutung im Sinne von Nummer 3 […] angenommen werden [kann], wenn die Aufklärungstätigkeit im Einklang mit dem sogenannten Auftragsprofil der Bundesregierung (APB) steht“.[15]

---

[15] BT-Drs. 18/9041 vom 05.07.2016, S. 34.

Offensichtlich wird jedoch mehr als der Schutz der nationalen Sicherheit bezweckt, andernfalls wäre keine explizite Nennung weiterer Zwecke neben der Aufklärung von „Gefahren für die innere und äußere Sicherheit“ notwendig gewesen. Selbst wenn angenommen wird, dass eine „Aufklärung von wirtschaftspolitisch bedeutsamen Vorgänge“ allein dem wirtschaftlichen Wohl des Landes i.S.v. Art. 8 Abs. 2 EMRK dienen soll, geht der Gesetzentwurf deutlich über die legitimen Zwecke hinaus, die die EMRK für Eingriffe in das Recht auf Privatsphäre vorsieht.

In Fragen nationaler Sicherheit räumt der EGMR den Vertragsstaaten der EMRK einen weiten Beurteilungsspielraum in der Frage ein, welche Mittel für welchen Zweck einzusetzen sind, fordert jedoch, dass Maßnahmen in gewissem Maße vorhersehbar sein müssen. Damit ist nicht gemeint, dass konkrete Einzelmaßnahmen für Zielpersonen antizipierbar sein müssen. Jedoch hat das nationale Recht in seinem Wortlaut hinreichend bestimmt zu sein, damit potenziell Betroffene angemessene Hinweise über Umstände und Bedingungen einer behördlichen Überwachung erhalten. Hierfür hat der Gerichtshof Mindestanforderungen an die „Qualität des Rechts“ aufgestellt, die er sowohl an Maßnahmen gezielter Überwachung wie an Programme strategischer Fernmeldeaufklärung anlegt.[16] Demnach müssen durch das Gesetz hinreichend detailliert bestimmt sein:

- die Art der Delikte, die zu Überwachungsanordnung führen können,
- die Kategorien von Personen, deren Kommunikation möglicherweise überwacht wird,
- die zeitliche Beschränkung der Überwachung,
- das Verfahren für die Auswertung, Verarbeitung und Speicherung von Daten,
- Sicherheitsvorkehrungen, die zu treffen sind, wenn Daten an Dritte übermittelt werden,
- die Umstände, unter denen gespeicherte Daten zu löschen sind.[17]

Der Gesetzentwurf enthält u.a. Vorgaben zur zeitlichen Beschränkung von Überwachungsanordnungen auf neun Monate (§ 9 Abs. 2 BNDG-E), zur Kennzeichnung und Löschung von Inhaltsdaten, die vom Inland aus erhoben wurden (§ 10 BNDG-E), sowie zum Kernbereichsschutz (§ 11 BNDG-E) und erfüllt damit einige der genannten Anforderungen.

Keine Angaben macht der Entwurf jedoch zur Art von sicherheitsbedrohlichem Verhalten oder den Kategorien von Personen, auf welche die strategische Überwachung gerichtet ist. Der EGMR anerkennt zwar die Notwendigkeit einer flexiblen Antwort auf sich wandelnde und schwer zu antizipierende Gefahren für die nationale Sicherheit und hat in seiner Rechtsprechung daher Forderungen nach detaillierten Deliktkatalogen in diesem Feld eine Absage erteilt. Gleichwohl mahnt er eine hinreichende Bestimmung dessen an, was unter Gefahren für die nationale Sicherheit zu verstehen ist.[18]

---

16 EGMR (2008): Liberty und andere gegen das Vereinigte Königreich, Rn. 63.
17 EGMR (2015): Roman Zakharov gegen Russland. Urteil vom 04.12.2015. Beschwerdenr. 47143/06, Rn. 227ff.
18 EGMR (2010): Kennedy gegen das Vereinigte Königreich, Rn. 159. Seine Kritik an der Offenheit des Begriffs „nationaler Sicherheit“ hat auch der UN-Menschenrechtsausschuss im Rahmen verschiedener Staatenprüfungsverfahren geäußert; siehe u.a. UN, Human Rights Committee (2016): Concluding observations on the sixth periodic report of New Zealand. UN Dok. CCPR/C/NZL/CO/6 vom 24.03.2016, Rn. 15.

Nicht abgemildert wird die fehlende Präzisierung im Gesetzentwurf durch die Begrenzung der Eingriffsvoraussetzungen im Falle von EU-Bürger_innen nach § 6 Abs. 3 BNDG-E oder das Verbot, Daten von Inländern zu erfassen. Die menschenrechtlichen Grenzen der Überwachung sind gegenüber EU-Bürger_innen und Drittstaatsangehörigen gleichermaßen einzuhalten. Befriedigen kann auch nicht die Einschränkung, dass die Erhebung von Daten nach § 6 Abs. 2 BNDG-E nur anhand von Suchbegriffen durchgeführt werden darf. Da die Suchbegriffe lediglich der Aufklärung der weit gefassten Sachverhalte dienen müssen und die technischen und organisatorischen Details nach § 6 Abs. 7 BNDG-E in einer Dienstvorschrift festgelegt werden sollen, die außerhalb der Exekutive nur dem Parlamentarischen Kontrollgremium zur Kenntnis zu geben ist, tragen sie nicht zur Präzisierung bei. Zudem gilt die Einschränkung der Datenerhebung durch Suchbegriffe nur für Inhaltsdaten nicht aber für Verkehrsdaten, die ohne Einschränkung erfasst und nach § 6 Abs. 6 BNDG-E für sechs Monate gespeichert werden dürfen. Damit kann potenziell jede_r Ausländer_in im Ausland, deren oder dessen Kommunikation über deutsche Knotenpunkte geleitet wird, von einer Erhebung und Analyse des Telekommunikationsverhaltens betroffen sein. Überdies ist es äußerst zweifelhaft, dass die Nichterfassung von Inländern durch ein mehrstufiges automatisches Filtersystem technisch realisierbar ist.[19]

Auch beim Betreiben eigener Überwachungsanlagen im Ausland, denkbar wäre dies zum Beispiel in Auslandsvertretungen oder militärischen Anlagen im Rahmen von multilateralen Stabilisierungsmissionen, würde der BND stabile Kontrolle über die Infrastruktur ausüben und wäre entsprechend zur Achtung der Menschenrechte verpflichtet. Allerdings vermeidet der Gesetzentwurf eine Klärung der Bedingungen und Voraussetzungen und nennt lediglich das Ausleiten von Daten im Ausland durch einen Telekommunikationsanbieter in der Begründung als mögliche Konstellation zu § 7 BNDG-E.[20] Welche Formen solch extraterritorialer Überwachung in „Public-Private-Partnership“ die Bedingung stabiler Kontrolle des BND über die Infrastruktur erfüllen, lässt sich hier nicht abschließend klären. Festzuhalten bleibt indes, dass die Datenerhebung des BND vom Ausland aus nach den Plänen des Gesetzentwurfs in jeder denkbaren Konstellationen weder inhaltlichen Beschränkungen unterliegt noch einer Anordnung durch das Bundeskanzleramt bedarf. Einzig ihre Weiterverarbeitung und Nutzung durch inländische Dienststellen soll Beschränkungen unterliegen. Eine Überwachung ihrer Kommunikation wäre für die Menschen in den betroffenen Regionen völlig unberechenbar.

Zusammengefasst erfüllt der Gesetzentwurf die menschenrechtlichen Anforderungen an eine rechtmäßige Kommunikationsüberwachung weder für die Fernmeldeaufklärung vom Inland noch vom Ausland aus. Eine Beschränkung der Überwachung auf die in der EGMR genannten legitimen Zwecke ist nicht gegeben, und das Gebot der Vorhersehbarkeit wird deutlich verfehlt.

Aus Sicht des Institutes sollten daher Eingriffe des BND in das Menschenrecht auf Privatsphäre sowohl im Inland als auch im Ausland auf Felder begrenzt werden, in denen sie im Sinne von Art. 8 Abs. 2 EGMR notwendig sind. Hierzu wäre es sinnvoll

---

[19] Greis, Friedhelm (2016): ECO warnt vor unkontrolliertem Zugriff auf deutschen Traffic. In: golem.de, 07.09.2016. http://www.golem.de/news/neues-bnd-gesetz-eco-warnt-vor-unkontrolliertem-zugriff-auf-deutschen-traffic-1609-123128.html,

[20] BT-Drs. 18/9041, S. 40.

sich auf die in § 6 Abs. 1 Nr. 1 genannten „Gefahren für die innere und äußere Sicherheit“ zu beschränken und durch die Nennung von zum Beispiel Phänomenbereichen oder Bedrohungslagen zu präzisieren. Weiterhin sollten auch die Erhebung und Verarbeitung von Verkehrsdaten begrenzt und Regelungen für die Kennzeichnung und Löschung von im Ausland erhobenen Daten getroffen werden.

## 3.2 Unabhängige und wirksame Kontrolle gewährleisten

Zu den menschenrechtlichen Anforderungen an die Rechtmäßigkeit einer Kommunikationsüberwachung gehört auch, dass ein wirksamer Rechtsschutz gegen willkürliche und rechtswidrige Eingriffe gewährleistet ist. Da bei heimlichen Maßnahmen, über die Betroffene häufig auch nach ihrer Beendigung keine Kenntnis erhalten, ein individueller Rechtsschutz kaum möglich ist, sind ersatzweise Verfahren zu etablieren, die „adäquate und gleichwertige Garantien“ zum Schutz der Betroffenenrechte gewährleisten. Normalerweise, so der EGMR, sollte diese Kontrolle durch Richter_innen wahrgenommen werden, welche Garant der notwendigen Unabhängigkeit, Unparteilichkeit und eines angemessenen Verfahrens sind. Den menschenrechtlichen Anforderungen genügen jedoch auch quasi-gerichtliche Ersatzverfahren wie die G 10-Kommission. Diese müssen unabhängig von den zu kontrollierenden Behörden und mit ausreichenden Vollmachten und Fähigkeiten für die Aufsicht ausgestattet sein.[21]

Nach § 16 BNDG-E soll ein „Unabhängiges Gremium“ zur Aufsicht über die Ausland-Ausland-Fernmeldeaufklärung des BND eingerichtet werden. Anders als die G 10-Kommission soll dieses Gremium nicht bei allen Maßnahmen für die Prüfung der Anordnungen zuständig sein, sondern nach § 9 Abs. 4 i.V.m. § 6 Abs. 1 BNDG-E nur, wenn es um die Bestimmung der zu überwachenden Telekommunikationsnetze geht, und nach § 9 Abs. 5 i.V.m. § 6 Abs. 2 BNDG-E bei der Wahl der Suchbegriffe, soweit sich diese auf EU-Einrichtungen und Behörden der Mitgliedstaaten beziehen. Daneben soll das Gremium gemäß § 9 Abs. 5 BNDG-E jederzeit stichprobenartig die Einhaltung der Vorgaben zur Verwendung von Suchbegriffen nach § 6 Abs. 3 BNDG-E überprüfen dürfen, d.h. nicht nur, wenn es um die Überwachung von europäischen Behörden geht, sondern auch um Bürger_innen der EU geht. Keinerlei Aufsichtsbefugnisse hat das Gremium im Feld der Überwachung von Menschen außerhalb der EU. Die umfassende Kompensation des fehlenden individuellen Rechtsschutzes für Ausländer_innen im Ausland ist durch das Unabhängige Gremium somit nicht gegeben; rechtlicher Schutz gegen willkürliche oder rechtswidrige Eingriffe in das Recht auf Privatsphäre nach Art. 17 Abs. 2 IPbpR wird zumindest für Nicht-EU-Bürger_innen verfehlt.

Angesichts der deutlichen Präferenz des EGMR für die richterliche Kontrolle nachrichtendienstlicher Maßnahmen ist die geplante Besetzung des Gremiums mit zwei Richter_innen des Bundesgerichtshofs aus menschenrechtlicher Perspektive positiv zu bewerten. Trotzdem wäre die Unabhängigkeit des Gremiums dauerhaft infrage gestellt: Wenngleich die Mitglieder bei der Ausübung ihrer Tätigkeit weisungsfrei sein sollen, ist geplant, dass sie von der Bundesregierung und nicht vom Parlament berufen werden. Zudem sieht der Gesetzentwurf vor, dass ein Mitglied des Gremiums eine Bundesanwältin oder ein Bundesanwalt wird und damit eine_n Vertreter_in der Exekutive. Das Vorschlagsrecht für diesen Posten läge beim

---

[21] EGMR (1978): Klass und andere gegen Deutschland, Rn. 55f.

Generalbundesanwalt, der als politischer Beamter dazu verpflichtet ist, dass er seine Aufgaben „in fortdauernder Übereinstimmung mit den für ihn einschlägigen grundlegenden kriminalpolitischen Ansichten und Zielsetzungen der Bundesregierung“ erfüllt.[22]

Angesichts der Komplexität moderner SIGINT ist fraglich, ob eine wirksame Kontrolle durch das Gremium in seiner geplanten Form gewährleisten werden kann. Seine drei Mitglieder sollen sich nach § 16 Abs. 4 BNDG-E neben ihrer Hauptbeschäftigung mindestens einmal im Quartal treffen. Die Sitzungsteilnahme der Stellvertreter_innen ist, anders als bei der G 10-Kommission, wo Stellvertreter_innen nach § 15 Abs. 1 G10 mit Rede- und Fragerecht an den Sitzungen teilnehmen können, nur vorgesehen, wenn ein Mitglied verhindert ist, so dass immer nur zu dritt getagt werden könnte. Nach § 16 Abs. 3 BNDG-E ist dem Gremium die notwendige Personal- und Sachausstattung zur Verfügung zu stellen. Geplant sind laut Gesetzentwurf insgesamt 15 Planstellen/Stellen für die Mitglieder des Gremiums, ihr Unterstützungspersonal und die Geschäftsstelle beim Bundesgerichtshof in Karlsruhe.[23] Obwohl das Gremium nicht nur die Zulässigkeit und Notwendigkeit von Anordnungen, sondern auch die Einhaltung der Vorgaben, wenngleich stichprobenartig, prüfen soll, fehlen ihr Frage-, Akteneinsichts- und Inspektionsrechte, wie sie die G 10-Kommision nach § 15 Abs. 5 G10 und § 110 Abs. 1 Nr. 5 TKG hat. Ebenfalls nicht vorgesehen ist besonderer technischer Sachverstand der Mitarbeiter_innen des Gremiums oder die Möglichkeit datenschutzrechtliche Expertise bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) anzufragen.

Überdies wäre ausgerechnet das Gremium, das Teile des „Kerngeschäfts“ des BND beaufsichtigen soll, durch den geplanten Sitz in Karlsruhe von den Gremien der Nachrichtendienstaufsicht in Berlin weitgehend isoliert. Nur dem Parlamentarischen Kontrollgremium soll nach § 16 Abs. 6 BNDG-E alle sechs Monate Bericht erstattet werden. Des Teilnahme des „Ständigen Bevollmächtigten“ des Kontrollgremiums, der durch die Novelle des PKGrG geschaffen werden soll, an Sitzungen des Unabhängigen Gremiums ist nicht geplant, obwohl dieser nach dem Willen der Koalition künftig Brücke und Schnittstelle zwischen den drei Aufsichtsgremien in Berlin sein soll.

In der Summe ist das Unabhängige Gremium, das den fehlenden individuellen Rechtsschutz nur für einen kleinen Teil der von der Ausland-Ausland-Aufklärung des BND betroffenen Personen, namentlich EU-Bürger_innen, und dann auch nur *ex post* durch Stichproben kompensieren könnte, wenig geeignet, die menschenrechtlichen Vorgaben an eine unabhängige und wirksame Aufsicht über nachrichtendienstliche Tätigkeiten zu erfüllen.

Wäre eine reformierte parlamentarische Kontrolle besser geeignet, die Arbeit der Nachrichtendienste zu kontrollieren? Aus demokratietheoretischer Sicht ist eine Stärkung der Minderheitenrechte in einem Feld, dem das Instrument demokratischer Öffentlichkeit weitgehend fehlt, grundsätzlich zu begrüßen. Angesichts nachvollziehbarer Sorgen vor einer parteipolitischen Instrumentalisierung müssten die

---

[22] Der Generalbundesanwalt: Rechtliche Stellung des Generalbundesanwalts beim Bundesgerichtshof, http://www.generalbundesanwalt.de/de/stellung.php.

[23] BT-Drs. 18/9041, S. 3.

Quoren und Mittel, die für eine wirksame und sachliche parlamentarische Kontrolle notwendig wären, eingehend diskutiert werden.

Zu bedenken ist aus Sicht des Institutes dabei jedoch, dass die parlamentarische Kontrolle die Kompensation des weitgehend fehlenden Rechtsschutzes gegenüber nachrichtendienstlichen Maßnahmen durch quasi-gerichtliche Kontrollinstanzen nicht ersetzen kann, da ansonsten eine Vermischung der Gewalten droht. Selbst bei einer von die Fraktion DIE LINKE. angestrebten Beendigung der nachrichtendienstlichen Kommunikationsüberwachung und des Einsatzes von V-Leuten bliebe die offene Frage ungeklärt, wie gegenüber anderen Maßnahmen verdeckter Informationserhebung wie etwa längere Observationen oder intransparenter Datenverarbeitung etwa durch wie „Big Data“-Analyseprojekte ein effektiver Rechtsschutz garantiert werden sollte.

Eine erste Möglichkeit wäre die Ausweitung der Zuständigkeiten der G 10-Kommission, was angesichts des sukzessiven Erweiterung ihrer Aufgaben im Laufe der letzten Jahre konsequent wäre. Sie könnte statt des geplanten „Unabhängigen Gremiums“ auch die Kontrolle der Ausland-Ausland-Überwachung des BND übernehmen. Zusätzlich könnte sie sich besonderen Formen der Datenerhebung annehmen, für die nach § 9 Abs. 3 BVerfSchG bislang weder ein Richtervorbehalt noch eine quasi-gerichtliche Kontrolle vorgesehen sind. Dabei wäre allerdings eine Professionalisierung der bislang ehrenamtlich arbeitenden Mitglieder der Kommmission zwingend geboten. Weiterhin könnte diskutiert werden, ob eine Professionalisierung mit der Festlegung spezifischer Kriterien zur Auswahl ihrer Mitglieder eingehen sollte.

Eine zweite Option wäre die Variation des geplanten Unabhängigen Gremiums als Kontrollorgan nicht nur für die Ausland-Ausland-Überwachung des BND mit Aufsichtsbefugnissen, die denen der G 10-Kommission vergleichbar sind. Denkbar wäre ein wirklich unabhängiges Gremium als allein mit Richter_innen besetztes Kontrollorgan, dessen Mitglieder vom Parlament oder dem Parlamentarischen Kontrollgremium bestimmt werden.

Für beide Optionen wäre eine deutliche Aufstockung des Unterstützungspersonals notwendig, inklusive der Gewährleitung, dass ausreichend technischer Sachverstandes vorhanden ist. Problematisch wäre es in jedem Fall, wenn die quasi-gerichtliche Kontrolle in Abhängigkeiten vom Kontrollgremium der Legislative geriete, wie es sich mit den Plänen der Koalition abzeichnet, den Mitarbeiterstab der G 10-Kommission nach § 12 Abs. 2 und 3 PKGrG-E der Dienst- und regelmäßigen Weisungsaufsicht der oder des geplanten Ständigen Bevollmächtigten zu unterstellen.

Für die Stärkung einer wirksamen Kontrolle unbedingt sinnvoll ist der Austausch der verschiedenen Aufsichtsgremien, inklusive ausgewählter Bundestagsausschüsse und Kontrollgremien der Länder, und die Einbeziehung der BfDI. Sie würde helfen, die Fragmentierung der Kontrolle zu verringern. In diesem Zusammenhang sind die Vorschläge sowohl der Koalitions- als auch Oppositionsfraktionen zu begrüßen, dass Sachverständigen-Berichte des Kontrollgremiums an Untersuchungsausschüsse und die Kontrollinstanzen der Landtage weitergeben werden können sollen. Positiv zu vermerken ist für die Verbesserung der vernetzten Aufsicht auch, dass offensichtlich im Rahmen der anstehenden Umsetzung der EU-Datenschutzreform die BfDI eine

gesetzliche garantierte Befugnis für die Prüfung auch von G 10-Daten erhalten soll,[24] wie sie seit dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei auf der datenschutzrechtlichen Tagesordnung steht.

Geprüft werden könnte bei einer grundlegenden Reform des Kontrollarchitektur auch, ob nicht eine klare Trennung der Zuständigkeiten zwischen der *ex ante*-Genehmigung von heimlichen Maßnahmen durch ein Gremium der quasi-richterlichen Kontrolle und einer *ex post*-Kontrolle durch die Datenschutzbeauftragte sinnvoll wäre. Gestrichen werden sollte in jedem Fall die Staatswohlklausel in § 24 Abs. 4 BDSG, da sie, wie die Vorgänge um die Prüfungen in Bad Aiblingen gezeigt haben, einer effektiven Aufsicht durch die BfDI im Wege steht.

## 3.3 „Vernetzte Sicherheit“ erfordert neue Formen der Kontrolle

Mit dem Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des BND sollen auch internationale Kooperationen des BND rechtlich geregelt werden. Dabei geht es um gemeinsame SIGINT-Projekte (§§ 13 bis 15 BNDG-E) und gemeinsame Dateien (§§ 26 bis 30 BNDG-E) mit ausländischen Partnern.

Mit dem Paradigmenwechsel vom „need to know“ to „need to share“ und der wachsenden Zusammenarbeit von Nachrichten- und Sicherheitsdiensten gehört die Kontrolle solcher Kooperationen zu den zentralen Herausforderungen für die gegenwärtige Aufsicht von Nachrichtendiensten. Mittlerweile hat das Thema auch den UN-Menschenrechtsausschuss erreicht. In seinen Abschließenden Bemerkungen zum jüngsten Staatenbericht Schwedens zeigte er sich in Bezug auf die SIGINT-Aktivitäten des Militärnachrichtendienstes FRA „besorgt über den Mangel an ausreichenden Garantien zum Schutz gegen willkürliche Eingriffe in das Recht auf Privatsphäre beim Austausch von Rohdaten mit anderen Nachrichtendiensten“ und empfahl die Einrichtung „effektiver und unabhängiger Aufsichtsmechanismen über den nachrichtendienstlichen Austausch von personenbezogenen Daten“.[25] Zuvor hatte der Ausschuss das Thema schon in seinen Abschließenden Bemerkungen zum Staatenbericht des Vereinigten Königreichs adressiert und zu einer „robusten“ Aufsicht geraten.[26]

Im Fall der geplanten SIGINT-Kooperationen des BND sollen nach § 13 Abs. 3 BNDG-E die Einzelheiten in einer schriftlichen Absichtserklärung niedergelegt werden. U.a. soll diese Erklärung Absprachen zur Zweckbindung der ausgetauschten Daten und der Vereinbarkeit ihrer Verwendung mit grundlegenden rechtstaatlichen Prinzipien beinhalten. Eine ähnliche Formel findet sich in den geplanten Vorschriften zu gemeinsamen Dateien. Nach § 26 Abs. 2 Nr. 2 BNDG-E sind solche Dateien nur zulässig, wenn in den teilnehmenden Staaten die Einhaltung grundlegender rechtsstaatlicher Prinzipien gewährleistet ist. Allerdings ist die Einhaltung rechtsstaatlicher Prinzipien nach § 26 Abs. 4 BNDG-E dabei nicht in den ebenfalls vorgeschriebenen Absichtserklärungen schriftlich zu fixieren, sondern nur die Zwecke der Zusammenarbeit und die Zusage, die übermittelten Daten ausschließlich in diesem Sinne zu verwenden, sowie das Auskunftsrecht des BND gegenüber seinen Partnern.

---

[24] § 25 Abs. 4 des öffentlich gewordenen Referentenentwurfs des BMI, Stand: 05.08.2016.
[25] UN, Human Rights Committee (2016): Concluding observations on the seventh periodic report of Sweden. UN Dok. CCPR/C/SWE/CO/7 vom 23.03.2016, Rn. 36f.
[26] UN, Human Rights Committee (2015): Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland. UN Dok. CCPR/C/GBR/CO/7 vom 21.07.2015, Rn. 24c.

Grundsätzlich sind die „Rechtsstaatlichkeitsklauseln“ zu begrüßen. Die wirksame externe Kontrolle ihrer Umsetzung ist aber fraglich. Den Absichtserklärungen für SIGINT-Kooperationen soll das Bundeskanzleramt zustimmen und das Parlamentarische Kontrollgremium ist über sie zu unterrichten. Auch im Fall der gemeinsamen Dateien ist die Zustimmung des Kanzleramts für die Zusammenarbeit einzuholen; das Kontrollgremium ist zu unterrichten. Unklar bleibt nach dem Wortlaut des Gesetzentwurfs, ob dies auch die Zustimmung zu den Absichtserklärungen beinhaltet. Bei beiden Formen der internationalen Kooperation würde es im laufenden Betrieb allein dem BND obliegen, bei den Partnerdiensten um Auskunft über die Verwendung der Daten zu ersuchen.

Bei den SIGINT-Kooperationen sollen BND-Mitarbeiter_innen stichprobenartig prüfen, ob durch die von Partnerdiensten gesteuerten Suchbegriffe grundrechts- und politisch sensible Daten erhoben und ins Ausland weitergegeben werden oder ob bei den vollautomatisierten Filter-, Lösch- und Übermittlungsroutinen alles mit rechten Dingen zugeht. Analog hierzu wird auch dem Unabhängigen Gremium nach § 15 Abs. 3 BNDG-E das Recht eingeräumt, die Einhaltung der Vorgaben stichprobenartig zu prüfen. Die Datenübermittlung selbst soll durch die BfDI geprüft werden können; flankierende Protokollierungspflichten sind in § 15 Abs. 2 BNDG-E vorgeschrieben. Eine Vorabkontrolle der durch ausländische Dienste beim BND gesteuerten Suchbegriffe ist weder intern noch extern vorgesehen und wäre angesichts der Datenmassen wohl auch nicht realisierbar. Im Überwachungsalltag bliebe die wirksame Kontrolle der Zuverlässigkeit der Maschinen überlassen, was vor dem Hintergrund des Wissens um die unzureichende Treffsicherheit der Filter nicht befriedigen kann.

Problematisch gestaltet sich auch die geplante externe Aufsicht im Hinblick auf die gemeinsamen Dateien des BND mit ausländischen Partnerbehörden. Hier ist für die Errichtung gemeinsamer Dateien beim BND vorgeschrieben, dass detaillierte Dateianordnungen mit Zustimmung des Bundeskanzleramtes und unter Anhörung der BfDI zu treffen sind. Wenn sich der BND hingegen an Dateien ausländischer Partner beteiligen würde, entzieht sich die Zusammenarbeit der datenschutzrechtlichen Kontrolle. Außer der oben genannten Absichtserklärung bedarf es nach § 30 BNDG-E keiner weiteren Dokumentation zu den Details der informationellen Kooperation oder ihrer Protokollierung. Selbst dem Kontrollgremium wären in diesem Fall weitgehend die Hände gebunden, da es von der Bundesregierung nach § 6 Abs. 1 PKGrG nur über Informationen und Gegenstände, die der Verfügungsberechtigung der Nachrichtendienste des Bundes unterliegen, unterrichtet werden muss.

Die „third party rule“, die den BND und die anderen deutschen Nachrichtendienste daran bindet, Informationen, die sie von ausländischen Partner erhalten haben, nicht an Dritte weiterzugeben, steht einer wirksamen Kontrolle der internationalen Kooperation entgegen. Entsprechend empfehlen verschiedene internationale Menschenrechtsgremien, dass der Zugang der Kontrolleure zu Informationen nicht am Veto ausländischer Behörden scheitern darf.[27] Vor diesem Hintergrund sind die Pläne der Koalition, bei einer Novelle des PKGrG dem Kontrollgremium das Recht einzuräumen, Konsultationsverhandlungen der Bundesregierung mit den

[27] Commissioner for Human Rights (2015): Democratic and effective oversight of national security services, . CommDH/IssuePaper(2015)2. Council of Europe. Strasbourg (Issue Paper), S. 13f.

ausländischen Partnern über die Freigabe von Informationen zu erzwingen, ein Fortschritt. Der menschenrechtlichen Verpflichtung, eine wirksame Kontrolle der Nachrichtendienste zu gewährleisten, genügen sie jedoch nicht.

Die Beispiele Belgien, Niederlande und Norwegen zeigen, dass es auch anders geht und es Aufsichtsgremien gibt, die zumindest im Prinzip nicht als „third party“ gelten.[28] Wie sich solche Vorbilder auf das deutsche Modell übertragen ließen, sollte geprüft werden. Diskutiert werden sollte auch, ob sich die Vorschläge, Sachverständigen-Berichte des Kontrollgremiums auch für eine Weitergabe an Untersuchungsausschüsse und Landtags-Kontrollgremien freizugeben, in relevanten Fällen auch auf ausländische Aufsichtsorgane anwenden ließen. Um mit der internationalen Kooperation der Dienste Schritt zu halten, sind dringend neue Wege gefordert.

**Kontakt**

Deutsches Institut für Menschenrechte
Zimmerstraße 26/27, 10969 Berlin
Tel.: 030 25 93 59-0
Fax: 030 25 93 59-59
info@institut-fuer-menschenrechte.de
www.institut-fuer-menschenrechte.de

AUTOR_IN: Eric Töpfer



**Das Institut**

Das Deutsche Institut für Menschenrechte ist die unabhängige Nationale Menschenrechtsinstitution Deutschlands. Es ist gemäß den Pariser Prinzipien der Vereinten Nationen akkreditiert (A-Status).
Zu den Aufgaben des Instituts gehören Politikberatung, Menschenrechtsbildung, Information und Dokumentation, anwendungsorientierte Forschung zu menschenrechtlichen Themen sowie die Zusammenarbeit mit internationalen Organisationen. Es wird vom Deutschen Bundestag finanziert. Das Institut ist zudem mit dem Monitoring der Umsetzung der UN-Behindertenkonvention und der UN-Kinderrechtskonvention betraut worden und hat hierfür entsprechende Monitoring-Stellen eingerichtet.

[28] van Laethem, Wauter (2011): Parliamentary and specialised oversight of security and intelligence agencies in Belgium. In: Parliamentary oversight of security and intelligence agencies in the European Union. European Parliament. Brussels (LIBE Study, PE 453.207), S. 191–203 (S. 199); Verhoeven, Nick (2011): Parliamentary and specialised oversight of security and intelligence agencies in the Netherlands. In: Parliamentary oversight of security and intelligence agencies in the European Union. S. 254–264 (S. 260). Norwegian Parliamentary Oversight Committee (2013), Abbreviated Annual Report for 2013, Oslo, S.1. https://eos-utvalget.no/english_1/annual_reports/content_3/text_1401199189882/1403522809228/forkortet_rsmelding_engelsk_versjon.pdf.