



THOMAS OPPERMAN
VORSITZENDER
DER SPD-BUNDESTAGSFRAKTION



CHRISTIAN FLISEK
SPRECHER DER ARBEITSGRUPPE ZUM
1. UNTERSUCHUNGSAUSSCHUSS („NSA“)



BURKHARD LISCHKA
SPRECHER DER ARBEITSGRUPPE INNERES
MITGLIED DES PARLAMENTARISCHEN KONTROLLGREMIIUMS

BERLIN, 16. JUNI 2015

Rechtsstaat wahren – Sicherheit gewährleisten!

Erste Konsequenzen aus dem NSA-Skandal: Eckpunkte der SPD-Bundestagsfraktion für eine grundlegende Reform der Strategischen Fernmeldeaufklärung des BND mit internationaler Vorbildwirkung

I.) Unser Zwischenfazit im Untersuchungsausschuss: Dringender Reformbedarf!	4
1.) Globale digitale Kommunikation kennt keine Ländergrenzen.....	4
2.) Auslands-Fernmeldeaufklärung des BND im rechtlichen Graubereich ohne ausreichende Kontrolle	4
3.) Probleme bei der Weiterleitung von Daten durch den BND an Partnerdienste.....	5
4.) Probleme bei der Datenerfassung und -verarbeitung durch den BND im Inland	5
II.) Rahmenbedingungen einer Reform der Rechtsgrundlagen des BND	6
1.) Wir brauchen leistungsstarke Nachrichtendienste!.....	6
2.) Das Fernmeldegeheimnis endet nicht an Deutschlands Grenzen!	7
3.) Internationale Signalwirkung schafft Vertrauen!	7
4.) Rechtliche Grenzen ziehen – Verhältnismäßigkeit wahren!	8
5.) Eine massiv gestärkte G10-Kommission als effektive Kontrollinstanz!	8
III.) Konkrete Eckpunkte der SPD-Bundestagsfraktion für eine grundlegende Reform der Strategischen Fernmeldeaufklärung des BND.....	9
1.) Befugnisnorm und Verbot nachrichtendienstlicher Vorratsdatenspeicherung.....	9
2.) Voraussetzungen und Beschränkungen der Erfassung von Routineverkehr.....	10
3.) Zentrale Einbeziehung einer neu strukturierten G10-Kommission.....	12
4.) Datenschutz umfassend gewährleisten.....	15

Edward Snowden hat im Sommer 2013 durch Veröffentlichungen, die auf von ihm entwendete Materialien des US-amerikanischen Nachrichtendienstes „National Security Agency“ (NSA) zurückgehen, gezeigt, in welchem Ausmaß Nachrichtendienste der „Five Eyes“-Staaten offenbar seit Jahren die **private, geschäftliche und politische Kommunikation in Europa und in der ganzen Welt ausspähen**.

Dies hat nicht nur zu einer Belastung der deutsch-amerikanischen Beziehungen geführt, sondern ist auch Ausgangspunkt einer **längst überfälligen Debatte über nationale und internationale Regeln für das neue Zeitalter globaler Kommunikationsstrukturen**, in welchem Nachrichtendienste in Anbetracht einer stetig wachsenden globalen Gefahrenlage eine immer größere Rolle spielen.

Als weltweit einziges Parlament hat der Deutsche Bundestag am 18. März 2014 hierzu einen **Untersuchungsausschuss mit einem umfassenden Aufklärungsauftrag** eingesetzt, der vor allem auch die **Deutschlandbezüge dieses internationalen Skandals** offenlegen soll. Der Untersuchungsausschuss hat in seinen bislang 53 Sitzungen rund 50 Zeugen mehr als 200 Stunden lang befragt und 13 Sachverständige angehört sowie inzwischen bereits rund über 2.100 Aktenordner Beweismaterial beigezogen und ausgewertet.

Der bisherigen gründlichen Arbeit dieses Ausschusses ist die Erkenntnis zu verdanken, dass auch die **Kooperation des Bundesnachrichtendienstes (BND) mit Nachrichtendiensten der „Five Eyes“-Staaten**, insbesondere mit der NSA, in einigen Aspekten als **äußerst problematisch** bewertet werden muss.

Erst ein Beweisbeschluss des Ausschusses brachte es im April 2015 ans Licht: Der BND hat im Rahmen einer in Kooperation mit der NSA durchgeführten Satellitenüberwachung in Bad Aibling über Jahre hinweg **Suchbegriffe („Selektoren“) der NSA nicht oder nicht ausreichend geprüft**. In das Suchprofil der Fernmeldeaufklärung von Satellitenkommunikation aus Krisenregionen wurden offensichtlich auch Begriffe eingestellt, die einer deutsch-amerikanischen Vereinbarung aus dem Jahre 2002 (*Memorandum of Agreement*) widersprachen und deutsche Interessen verletzen.

Die Beweisaufnahme des Ausschusses offenbarte dabei **schwere technische und organisatorische Defizite im BND**, die inzwischen auch von BND-Präsident Schindler und vom Bundeskanzleramt eingeräumt worden sind.

Schon bei der ersten **Anhörung von Verfassungsrechtsexperten** durch den Ausschuss im Mai 2014 war deutlich geworden, dass sich der BND bei der Überwachung ausländischer Telekommunikation in einer **rechtlichen Grauzone** bewegt. Es fehlen ausreichende gesetzliche Grundlagen. Besonders problematisch ist dies, wenn die Erfassung solcher Kommunikation durch Kabelzugriffe im Inland erfolgt (Stichwort: „*Eikona*“). Zudem wurde mit zweifelhaften regierungsinternen Gutachten (Stichwort: „*Weltraumtheorie*“) jahrelang die Anwendung deutschen Datenschutzrechts für diesen Bereich umgangen.

Der „Selektoren-Skandal“ hat gezeigt, dass im BND zwar offenbar die Beachtung des Gesetzes zu Artikel 10 Grundgesetz (G10) hohe Priorität genoss und der **Telekommunikationsverkehr deutscher Staatsbürger** deshalb penibel ausgefiltert und damit geschützt wurde. Aber für die Fernmeldeaufklärung *ausländischer* Staatsbürger im Ausland gab es kaum Beschränkungen. Hier war alles - so ein BND-Mitarbeiter aus Bad Aibling in seiner Vernehmung im Ausschuss wörtlich - „zum Abschuss freigegeben“.

Auch wenn mittlerweile in Politik und Wissenschaft an der Gesetzeslage vielfach Kritik geübt wurde, **mangelt** es bisher an **konkreten und praktikablen Vorschlägen** zur Abhilfe. Die Opposition erweckt den Eindruck, sie wolle die Strategische Fernmeldeaufklärung am liebsten ganz einstellen, CDU und CSU scheinen alles im bestehenden rechtlichen Graubereich belassen zu wollen. Die SPD ist momentan die einzige politische Kraft im Bundestag, die konkrete Vorschläge für eine aus unserer Sicht verfassungsrechtlich gebotene Reform vorlegt.

Die Reform darf auch nicht auf die lange Bank geschoben werden! Ein Zuwarten bis zum Ende der Legislaturperiode - oder gar darüber hinaus - ließe den verfassungsrechtlich problematischen Zustand zum vorsätzlichen Verfassungsbruch werden. Das Handeln des BND im Bereich der Auslandsaufklärung muss möglichst bald auf eine **glaubwürdige und verfassungsrechtlich einwandfreie gesetzliche Grundlage** gestellt werden! Die SPD-Fraktion stellt daher klare **Eckpunkte für eine grundlegende Reform** vor. Unsere **wichtigsten Forderungen** gegenüber dem Bundeskanzleramt:

- **Schließen der bestehenden gesetzlichen Regelungslücken** bei der Strategischen Fernmeldeaufklärung durch den BND.
- Maßnahmen dürfen nur im Rahmen des **Auftragsprofils der Bundesregierung für den BND** erfolgen. Sie müssen notwendig und verhältnismäßig sein und dürfen **nicht gegen deutsche Interesse verstoßen**.
- Bei Erstbeantragung einer Maßnahme muss **der BND-Präsident zustimmen**.
- **Verbot der Bildung eines „Daten-Heuhaufens“** nach Vorbild der NSA.
- Ausdrückliches **Verbot der Wirtschaftsspionage** zur Erlangung von Wettbewerbsvorteilen in kommerzieller Hinsicht.
- **Besonderer Schutz von EU-Bürgern, EU-Mitgliedstaaten und EU-Institutionen**.
- Gesetzliche Klarstellung der **Geltung der bestehenden Datenschutzbestimmungen auch für rein ausländische Kommunikation**, insbesondere bei der Übermittlung an ausländische Partnerdienste.
- Ausdrückliches **Verbot eines systematischen „Ringtauschs“** zur Umgehung nationaler Restriktionen. Konkrete Meldungen mit nachrichtendienstlicher Relevanz müssen aber selbstverständlich weiter ausgetauscht werden können.
- **Wirksame interne Kontrolle** durch verpflichtende Beteiligung des behördlichen G10-Juristen bei der Erfassung, Speicherung, Verarbeitung und Löschung von Daten.
- **Externe Kontrolle** der gesamten Fernmeldeaufklärung des BND durch eine **erweiterte und massiv gestärkte G10-Kommission**. Bereits existierende Kontrollbefugnisse der G10-Kommission müssen auf die gesamte Fernmeldeaufklärung **ausgeweitet** werden. Neue Kompetenzen, wie etwa die Möglichkeit, **Sachverständige einzusetzen**, müssen hinzukommen.
- **Verstärkte personelle Unterstützung der G10-Kommission** (juristisch, technisch, nachrichtendienstlich) bei der Wahrnehmung ihrer Aufgaben und Bestimmung eines **hauptamtlichen Datenschutzbeauftragten in der G10-Kommission**.

I.) Unser Zwischenfazit im Untersuchungsausschuss: Dringender Reformbedarf!

Die Beweisaufnahme im Untersuchungsausschuss hat einen **dringenden Handlungsbedarf** bei den gesetzlichen Grundlagen der Fernmeldeaufklärung des BND offengelegt:

1.) Globale digitale Kommunikation kennt keine Ländergrenzen

Das Grundrecht der Telekommunikationsfreiheit des Artikels 10 Grundgesetz (Art. 10 GG) bezog sich lange auf rein **analoge Kommunikationsmittel**, die territorial gebunden und ohne weiteres national abgrenzbar waren. Doch das hat sich - insbesondere in den letzten 20 Jahren - weltweit radikal geändert. Digitalisierung und Privatisierung der Telekommunikationsnetze haben **globale Kommunikationswege** zur Normalität werden lassen. Selbst nationale Telekommunikation spielt sich nicht mehr zwingend im territorialen Hoheitsgebiet der Bundesrepublik ab. Nicht nationale Grenzen, sondern die Wahl von Anbieter und Software entscheiden, welchen Weg digitale Pakete rund um den Erdball nehmen.

Die rechtliche Unterscheidung zwischen In- und Ausland verliert dadurch an Bedeutung. In Deutschland transportieren Telekommunikationsnetze in gleicher Weise Daten rein ausländischer Kommunikation, wie Kommunikation rein deutscher Teilnehmer im Ausland. Entscheidender wird die jeweilige **rechtliche Stellung** jener Personen, die Ausgangs- und Endpunkt des Kommunikationsvorgangs sind. Hier spielt auch die **europäische Einigung** eine besondere Rolle: Sie hat nicht nur die internationalen Kommunikationsnetze ermöglicht und befördert. Mit der EU sind auch ein gemeinsamer Rechtskreis und eine **Wertegemeinschaft** entstanden, die sich umfassend der Einhaltung wesentlicher Grund- und Menschenrechte verpflichtet hat.

2.) Auslands-Fernmeldeaufklärung des BND im rechtlichen Graubereich ohne ausreichende Kontrolle

Für die Erfassung von Telekommunikation im Ausland bzw. unter ausschließlicher Beteiligung von Ausländern gibt es bislang **keine klaren gesetzlichen Vorschriften**. Das ist nicht nur verfassungsrechtlich problematisch, sondern es **beschädigt auch das Vertrauen** der Bevölkerung in die Rechtmäßigkeit der Arbeit der Sicherheitsbehörden.

Telekommunikation ohne Beteiligung Deutscher oder ohne unmittelbaren Deutschlandbezug wird im BND-Jargon „**Routineverkehr**“ genannt. Nach Auffassung des BND ist dieser Routineverkehr dann nicht vom Grundrecht der Telekommunikationsfreiheit des Art. 10 GG geschützt, wenn beide ausländischen Teilnehmer sich nicht im deutschen Staatsgebiet aufhalten. Die Erfassung solcher Daten fände - gesetzlich ungeregelt - im „offenen Himmel“ oder - bei der Erfassung von Satelliten-Kommunikation - gar im „Weltraum“ statt. Die Daten seien deshalb, so ein BND-Mitarbeiter als Zeuge im Ausschuss, „zum Abschuss freigegeben“.

Der BND stützt sich für die Erhebung von Daten aus Routineverkehr allein auf die gesetzliche **Beschreibung seiner Aufgaben** im Gesetz über den Bundesnachrichtendienst (BNDG). Dessen Normen enthalten aber weder die ausdrückliche Befugnis, in Grundrechte wie Art. 10 GG einzugreifen, noch gibt es Bestimmungen, unter welchen Voraussetzungen und mit welchen Grenzen eine Erfassung von Routineverkehren vorgenommen werden darf. Genauso bleibt unbestimmt, welche **datenschutzrechtlichen Normen** bei der Speicherung, Verarbeitung und Weitergabe an Dritte zwingend anzuwenden sind.

3.) Probleme bei der Weiterleitung von Daten durch den BND an Partnerdienste

Symptomatisch für den Mangel an gesetzlichen Grundlagen ist der Skandal um das Einstellen **unzulässiger Selektoren** der NSA in das Suchprofil des BND in Bad Aibling. Es blieb offensichtlich in der Praxis völlig unklar, welche Suchbegriffe „**deutsche Interessen**“ verletzen konnten und nicht Gegenstand der Auswertung und Weiterleitung an die NSA sein durften. Eine Prüfung erfolgte viel zu spät und wurde nicht konsequent umgesetzt. Es gab im BND auch keine Regeln oder verlässliche Verfahren, wie außerhalb einer G10-Filterung die **Einhaltung bilateraler Absprachen** kontrolliert werden soll.

Derzeit werden nicht nur **Inhaltsdaten** aus der Satellitenüberwachung nach einer Selektion, sondern auch **Metadaten** - also strukturierte Daten *über* durchgeführte Kommunikationsverbindungen oder entsprechende Versuche - automatisiert an ausländische Nachrichtendienste weitergeleitet. Wenn man wie der BND einen **Deutschlandbezug** verneint („Weltraumtheorie“), wäre dies mangels gesetzlicher Grenzen unbeschränkt und unkontrolliert möglich, so lange keine Deutschen betroffen sind. Die Überleitungsvorschriften des BNDG gölten nicht.

Darüber hinaus sind Metadaten nach Ansicht des BND nur dann geschützt, wenn es sich um „**personenbezogene Daten**“ handelt. Dies wird bei einem Datum verneint, wenn im konkreten Fall ein Personenbezug nur unter großem Aufwand hergestellt werden kann. Eine solch **isolierte Betrachtung** ignoriert jedoch die Tatsache, dass Metadaten heute in einem größeren Kontext oder in Kombination mit weiteren hinzutretenden Informationen sehr schnell personenbeziehbar werden (Ex-NSA-Chef Michael Hayden: „*We Kill People Based On Metadata.*“).

Der BND wendet zwar ein, er habe in der Praxis schon immer **elementare Rechtsprinzipien** beachtet. Auch seien seine Datenbanken so konzipiert und programmiert, dass sie in vollem Umfang den strengen datenschutzrechtlichen Vorgaben des BNDG entsprächen. Die Beweisaufnahme des Untersuchungsausschusses hat jedoch ergeben, dass die **Rechtsanwendung** durch den BND in der nachrichtendienstlichen Praxis zu einer ganzen Reihe von **Folgeproblemen** führt, insbesondere wenn die Behörde im Inland und damit im Geltungsbereich des Grundgesetzes handelt.

4.) Probleme bei der Datenerfassung und -verarbeitung durch den BND im Inland

Der Zugriff auf den **kabelgebundenen Routineverkehr** im Inland ist nur in Kooperation mit den Netzbetreibern möglich. Ist auf den Kabelstrecken auch Kommunikation enthalten, die unter das G10 fällt, erfordert die Erfassung die Einholung einer **G10-Genehmigung**, auch wenn Erfassungsziel allein der Routineverkehr sein sollte.

Damit wird die G10-Genehmigung *de facto* zum „Türöffner“ für die Erfassung von Routineverkehr, weil die Netzbetreiber zur Bereitstellung eines vollständig gespiegelten Übertragungsweges, also sämtlicher auf diesen Kabelstrecken vorhandenen Kommunikationsinhalte, verpflichtet sind. Auch wenn die hierbei gewonnenen G10-Daten im Rahmen des G10 verarbeitet werden, so bleibt das **Dilemma**: Das Gesetz verbietet nicht den Zugriff auf Routineverkehr im Inland – es erlaubt aber auch keinen Zugriff darauf. Die G10-Anordnung wird erwirkt, um (auch) Aufgaben außerhalb des G10 und damit **außerhalb** seiner **gesetzlichen Zwecke** wahrzunehmen. Es fehlt dem BND also eigentlich ein konkretes rechtliches Instrument, um reinen Routineverkehr bei Telekommunikationsunternehmen in Deutschland erfassen zu dürfen.

II.) Rahmenbedingungen einer Reform der Rechtsgrundlagen des BND

1.) Wir brauchen leistungsstarke Nachrichtendienste!

Die SPD-Bundestagsfraktion betont ausdrücklich die **Notwendigkeit von Nachrichtendiensten** zur Gewährleistung unserer inneren und äußeren Sicherheit. Die Bundesrepublik Deutschland muss ihre Außen- und Sicherheitspolitik und ihre internationale Zusammenarbeit auf Vorgänge im Ausland einstellen können und bedarf hierfür auch im Interesse ihrer **Handlungs- und Bündnisfähigkeit** entsprechender Kenntnisse. Zudem hat der BND wichtige Aufgaben im Bereich der Gefahrenabwehr, der Terrorismusbekämpfung und des Schutzes von Leib und Leben der im Ausland eingesetzten deutschen und alliierten Streitkräfte („**Force Protection**“).

Hier ist regelmäßig der **Schutz hochrangiger Gemeinschaftsgüter** betroffen, deren Verletzung schwere Schäden für den äußeren und inneren Frieden und die Rechtsgüter Einzelner zur Folge hätte. Die Bedrohung durch die Terrorgruppe Islamischer Staat (IS) ist beispielsweise hochaktuell und hat auch unmittelbare Auswirkungen auf die Gefahrenlage in Deutschland. Die Rückkehr von gewaltbereiten radikalisierten Kämpfern aus Syrien oder dem Irak stellt eine unmittelbare Bedrohung dar und erfordert fundierte nachrichtendienstliche Erkenntnisse, um wirksame Gegenmaßnahmen treffen zu können. Insgesamt leistet der BND durch seine Arbeit unverzichtbare Beiträge zum Schutz von Menschenleben im In- und Ausland.

Dabei ist die **vertrauensvolle, rechtlich gebundene und wirksam kontrollierte Kooperation mit Nachrichtendiensten befreundeter Staaten** unverzichtbar. Vor allem der technologische Austausch mit den US-Diensten ist für den BND und die Sicherheit Deutschlands von vitalem Interesse.

Die Dienste haben aber zugleich die **rechtsstaatlichen Grenzen** und die Freiheitsgarantien unseres Grundgesetzes strikt zu wahren. Freiheitsrechte dürfen nicht abstrakten Sicherheitsinteressen geopfert werden. Jeder Eingriff in die Bürgerrechte bedarf einer **Rechtfertigung** in Gestalt einer umsichtigen **Güterabwägung**. Entsprechende Kontrollgremien müssen dies auch im Einzelfall sicherstellen.

Die bisherige Beweisaufnahme des Untersuchungsausschusses hat gezeigt, dass der BND eine große Behörde mit gewichtigem und sehr spezifischem Auftrag ist, in der allerdings auch **Fehler** gemacht werden. Aber im BND werden **Recht und Gesetz** in gleicher Weise **geachtet** wie auch in anderen Behörden. Der Schutz der Grundrechte der Bürgerinnen und Bürger der Bundesrepublik Deutschland nimmt dabei großen Raum ein, Anhaltspunkte für einen rechtswidrigen „Ringtausch“, also eine wechselseitige Datenübermittlung befreundeter Dienste jeweils zur Umgehung der eigenen nationalen Restriktionen, sind bisher nicht ersichtlich. Viele kompetente Mitarbeiter des Dienstes haben als Zeugen zur Sachaufklärung beigetragen und hierbei gezeigt, dass sie die rechtlichen Grundlagen ihrer Arbeit durchaus ernst nehmen und reflektieren.

Der BND kann aber nur dann **gute Arbeit** leisten, wenn er auch auf einem gesicherten und stringenten rechtlichen **Fundament** steht. Das sind wir auch den weit über 6.000 BND-Beschäftigten schuldig. Nur dann besteht auch eine **ausreichende Legitimation** für ihre Tätigkeit.

2.) Das Fernmeldegeheimnis endet nicht an Deutschlands Grenzen!

Eine **Reform der Rechtsgrundlagen** muss unserer Verfassung Rechnung tragen. Die Fernmeldeaufklärung durch den BND greift auch dann in das **Grundrecht der Telekommunikationsfreiheit** des Art. 10 GG ein, wenn **nur Ausländer im Ausland** betroffen sind. Dies ergibt sich bereits aus konsequenter Weiterentwicklung der Verfassungsgerichtsrechtsprechung und der unmittelbaren Verpflichtung aller staatlichen Stellen aus Art. 1 Abs. 3 GG, die Grundrechte zu achten. Art. 10 GG entfaltet deshalb auch für den BND **weltweite Wirkungen**.

Dabei ist allerdings zu beachten, dass die Geltung eines Grundrechts **nicht auf der ganzen Welt gleich intensiv** ist. Die **Schutzwirkung** des Fernmeldegeheimnisses ist dort am stärksten, wo ein Mensch **unmittelbar und in vollem Umfang** der staatlichen Gewalt unterworfen ist, die in seine Rechte eingreift. Im Rahmen einer **Abwägung** mit den legitimen Sicherheitsinteressen sind daher die Nationalität der Kommunizierenden, der Ort der Erfassung der Kommunikation und der Ort ihrer Verarbeitung, Speicherung und Nutzung zu beachten.

Die Erfassung reiner Ausland-Auslands-Kommunikation durch den BND - egal ob im Inland oder im Ausland - ist von einer grundlegend anderen Sach- und Interessenlage gekennzeichnet als eine Inlandserfassung. Art. 10 GG darf deshalb in Abwägung mit den zu schützenden hochrangigen Rechtsgütern nicht eindimensional als auch im Ausland geltendes subjektives Abwehrrecht missverstanden werden. Es kann über Art. 1 Abs. 3 GG nur einen **objektiv-rechtlichen Schutzauftrag** entfalten.

Zu beachten sind zusätzlich die **Rechte von EU-Bürgern**: Im Gegensatz zu Staatsangehörigen aus anderen Ländern gilt hier die EU-Grundrechtecharta und die Eingriffsintensität der Überwachung ist durch die Rechtsharmonisierung in der EU stärker geworden. Der BND ist deshalb gesetzlich zu verpflichten, Telekommunikation aus Staaten außerhalb des Aufgabenprofils (wie EU-Staaten) nur in **eng beschränkten Fällen zur Gefahrenabwehr** (etwa: Terrorismus, Proliferation, Drogenhandel) zum Gegenstand der strategischen Aufklärung zu machen.

3.) Internationale Signalwirkung schafft Vertrauen!

Die Datenüberwachung durch Dienste anderer Staaten können wir nur dann **glaubwürdig** kritisieren, wenn wir international deutlich machen, dass wir unsere Dienste zur Einhaltung eines **Mindestmaßes an Menschenrechtsschutz** verpflichten. Sie sollen nicht massenhaft, willkürlich Daten von Ausländern im Ausland erheben, auch wenn sie es technisch können. Befreundete Staaten sollen nur dann das Ziel von Erfassungen sein, wenn dies das Auftragsprofil der Bundesregierung nicht von vorneherein verbietet und **konkrete Gefahrenbereiche** betroffen sind. Einen **Ringtausch** zur Umgehung nationaler Restriktionen wollen wir wirksam verhindern.

Damit können wir zugleich befreundete Staaten davon **überzeugen**, ihrerseits die Arbeit ihrer Nachrichtendienste auf Grundlagen zu stellen, die eine unbeschränkte Überwachung unserer Bürger ausschließt. Da es hier - beispielsweise in der EU - noch keine **internationalen Standards** gibt, sind solche im Weiteren anzustreben.

Damit verbessern wir zugleich mittelbar den **Grundrechtsschutz unserer Bürger**. Je mehr sich unsere Partner zu vergleichbaren gemeinsamen Standards für die nachrichtendienstliche Arbeit entschließen, umso weniger müssen unsere Bürgerinnen und Bürger befürchten, von den Diensten befreundeter Länder überwacht zu werden.

Dieser Schutz geht dann auch deutlich über **unverbindliche „No-Spy“-Abkommen**, die nach Aussage des BND-Präsidenten im Ausschuss in der von der damaligen Bundesregierung propagierten Form noch nicht einmal zwischen den „Five Eyes“-Staaten existieren, hinaus. Denn die Dienste würden nicht durch - mehr oder weniger schwammige - völkerrechtliche Vereinbarungen, sondern durch ihre **eigene nationale Rechtsordnung** und im nationalen Recht verankerte wirksame Kontrollmechanismen zur Beachtung deutscher Rechtsgüter verpflichtet.

4.) Rechtliche Grenzen ziehen – Verhältnismäßigkeit wahren!

Der BND muss in der Lage sein, das ihm von der Bundesregierung vorgegebene und parlamentarisch kontrollierte **Auftragsprofil** erfüllen zu können und den sicherheitspolitischen Interessen der Bundesrepublik Deutschland effektiv gerecht zu werden.

Andererseits ist die Schaffung einer bloßen Befugnisnorm für den BND nicht ausreichend, wenn sie alleine die Erfassung von Routineverkehr legitimieren soll. Wir müssen vielmehr **gesetzliche Grenzen** einer solchen Überwachung bestimmen. Die Erfassung ausländischer Kommunikation ist auf das erforderliche Maß zu beschränken. Daten, die nicht für die Aufgabenerfüllung notwendig sind, sind schnellstmöglich zu löschen. Statt eines möglichst großen Daten-Heuhaufens, wie ihn die NSA anstrebt, muss für den BND gelten: **So viel wie nötig und so wenig wie möglich**. Dazu sind die Daten unverzüglich zu separieren, zu selektieren und zu löschen, falls sie keine nachrichtendienstliche Relevanz besitzen.

5.) Eine massiv gestärkte G10-Kommission als effektive Kontrollinstanz!

Die Einhaltung der gesetzlich vorzusehenden Grenzen und Beschränkungen bei der Erfassung von Routineverkehren muss kontrolliert werden. Neben **internen Kontrollen** durch eigene **G10-Juristen** im BND ist die Erfassung von Routineverkehren durch den BND extern durch eine **unabhängige Kontrollinstanz** zu regulieren. Hier ist die **Einbeziehung der G10-Kommission** sachdienlich, da ihre bisherige Zuständigkeit bereits einen engen Bezug zur Fernmeldeüberwachung aufzeigt, ihre Mitglieder dem Geheimschutz verpflichtet sind und sie zugleich eng an die parlamentarische Kontrolle der Nachrichtendienste angebunden ist. Die G10-Kommission als unabhängige **quasi-richterliche Kontrollinstanz** hat sich bisher bewährt.

Die G10-Kommission und flankierend das Parlamentarische Kontrollgremium sind entsprechend durch Sachmittel und qualifiziertes Hilfspersonal der Bundestagsverwaltung zu unterstützen. Dieses ist **zwingend** aufzustocken und sollte neben juristischen auch technischen und nachrichtendienstlichen **Sachverstand** umfassen, so dass eine **umfassende, regelmäßige und effiziente Kontrolle** unter Beachtung der gesetzlichen Aufgaben ohne weiteres möglich ist. Spezielle **Organisations- und Verfahrensbestimmungen für die G10-Kommission** können die Kontrolle noch intensivieren.

III.) Konkrete Eckpunkte der SPD-Bundestagsfraktion für eine grundlegende Reform der Strategischen Fernmeldeaufklärung des BND

Wir fordern deshalb das Bundeskanzleramt auf, schnellstmöglich folgende **Eckpunkte einer Reform** der Strategischen Fernmeldeaufklärung von Telekommunikationsbeziehungen (**StraFmA**) von Teilnehmern, die nicht dem Gesetz zu Artikel 10 Grundgesetz (G10) unterfallen, durch den BND auf den Weg zu bringen, um eine **rechtsstaatlich einwandfreie, verfassungsrechtlich ausgewogene und international vorbildgebende gesetzliche Grundlage** hierfür zu schaffen:

1.) Befugnisnorm und Verbot nachrichtendienstlicher Vorratsdatenspeicherung

- Selbst große Gefahren für die Sicherheitsinteressen Deutschlands rechtfertigen Maßnahmen der Nachrichtendienste nicht ohne jegliche Voraussetzungen und Begrenzungen (vgl. nur: BVerfGE 100, S. 313, 383).

Es muss deshalb für die strategische Erhebung, Verarbeitung und Nutzung von Daten aus extranationalen, nicht § 5 G10 unterfallenden, Telekommunikationsverkehren ohne Deutschlandbezug („Routineverkehr“), über Vorgänge im Ausland von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland (Strategische Fernmeldeaufklärung-Routineverkehr, „**StraFmA-R**“) eine **mit normativen Vorgaben versehene klare Befugnisnorm** geschaffen werden. Diese - unverzichtbare - Tätigkeit des BND im Rahmen der Auslandsaufklärung ist aus dem gegenwärtig bestehenden rechtlichen Graubereich herauszulösen und der Anwendungsbereich, die Eingriffsvoraussetzungen und der Mitteleinsatz sind **eindeutig und limitierend zu regeln**.

Dabei ist vor allem den verfassungsrechtlichen Grundsätzen der **Achtung der Menschenwürde**, der **Verhältnismäßigkeit** und des **Willkürverbots** neben dem objektiv-rechtlichen Schutzauftrag des **Grundrechts der Telekommunikationsfreiheit des Art. 10 GG** sowie den vom Deutschen Bundestag ratifizierten **internationalen Konventionen** und den für Deutschland geltenden **Völkerrechtsnormen zum Schutz der Menschenrechte** (vgl. etwa: Art. 12 AEMR, Art. 8 EMRK, Art. 17 IPbpR etc.) Rechnung zu tragen.

- Es soll **gesetzlich ausgeschlossen** werden, ohne konkreten Anlass eine **langfristige Speicherung** der erfassten Inhaltsdaten der Telekommunikationsverkehre vorzunehmen. Es muss vor allem sichergestellt werden, dass Inhaltsdaten nicht unabhängig von ihrer im Einzelfall geprüften nachrichtendienstlichen Relevanz langfristig gespeichert werden. Die Bildung eines „**Massendaten-Heuhaufens**“ **ist zu verbieten**, wenn er als Grundlage für einen späteren Abgleich mit zum Zeitpunkt der Speicherung der Inhaltsdaten noch nicht erkannten Suchbegriffen dienen soll.

Zulässig dürfte es jedoch bleiben, wenn der BND Fernmeldevorgänge durch Spiegelung bestimmter Kommunikationsstrecken (vgl. § 27 Abs. 2 TKÜV) allein technikbedingt zunächst miterfasst, sie aber unmittelbar nach Signalaufbereitung und Filterung technisch wieder **spurenlos aussondert**, weil hier - ohne Speicherung in Datenbanken oder Möglichkeit der Inaugenscheinnahme durch einen Auswerter - das Grundrecht aus Artikel 10 GG noch nicht tangiert ist (vgl. BVerfGE 100, S. 313, 366).

- Die Bundesregierung sollte im Rahmen der Neuregelung intensiv prüfen, ob für die **Erfassung von Metadaten**, bei denen es sich - im Gegensatz zu Inhaltsdaten *aus* einer durchgeführten Kommunikation - allein um strukturierte Daten *über* durchgeführte Kommunikationsverbindungen oder entsprechende Versuche handelt, **gesonderte Vorschriften** geschaffen werden sollten. Dabei muss Berücksichtigung finden, dass auch Metadaten aus Routineverkehr sehr wohl personenbezogene Daten im Sinne von § 3 BDSG sein können, etwa dann, wenn sie in Teilen deckungsgleich mit nachrichtendienstlich relevanten Suchbegriffen sind, die beispielsweise einzelnen konkreten Gefährdern im Ausland zugeordnet werden können.

In diese Überlegungen sollte aber einbezogen werden, dass hinsichtlich der Speicherung und Verarbeitung von Metadaten andere Vorgaben gelten können als beim Umgang mit Inhaltsdaten. Derartige Metadaten werden nicht nur nach bestimmten vorgegebenen Selektoren durchsucht, sie können vielmehr vor allem auch dazu dienen, durch besondere, automatisierte, technische Analyse neue Hinweise auf nachrichtendienstlich relevante Suchbegriffe zu erlangen (vgl. § 6 Abs. 3 G10). Hierbei ist jedoch sicherzustellen, dass bei der Speicherung von Metadaten **angemessen kurze Fristen** vorgesehen werden, um eine im Sinne der verfassungsgerichtlichen Rechtsprechung unverhältnismäßige Speicherung auch im Bereich der Metadaten von Routineverkehr auszuschließen.

2.) Voraussetzungen und Beschränkungen der Erfassung von Routineverkehr

- Für die Strategische Aufklärung von **Inlands-Auslands-Telekommunikation (StraFmA-G10)** muss weiter der Anwendungsbereich des § 5 G10 als die spezielle Regelung mit seinen hohen gesetzlichen Anforderungen gelten. Gleiches gilt auch für die §§ 3 und 8 G10.
- Bei der **Strategischen Aufklärung von Routineverkehr (StraFmA-R)** muss sichergestellt werden, dass diejenigen Vorgänge im Ausland, über die der BND Informationen erheben möchte, einen unmittelbaren **Bezug zum konkreten „Auftragsprofil der Bundesregierung für den BND“ (APB)** aufweisen oder im Zusammenhang stehen mit dem Schutz von Leib und Leben der in Krisenregionen eingesetzten deutschen und alliierten Streitkräfte („**Force Protection**“).

Letztlich muss jede Maßnahme dem **Schutz wesentlicher Sicherheitsinteressen der Bundesrepublik Deutschland** zu dienen bestimmt sein.

Das Bundeskanzleramt sollte gesetzlich verpflichtet werden, dieses Auftragsprofil für den BND **der G10-Kommission in geeigneter Form zur Kenntnis zu geben**, soweit es Grundlage für die jeweilige Maßnahme der StraFmA ist.

- Es muss gesetzlich klargestellt werden, dass vom BND keine Erkenntnisse über **Unternehmen der Privatwirtschaft** erhoben werden dürfen, die allein der Erlangung von Wettbewerbsvorteilen in kommerzieller Hinsicht zu dienen bestimmt sind („**Verbot der Wirtschaftsspionage**“).

- Die reformierten Rechtsgrundlagen für den BND müssen vorsehen, dass die ausgewählten Übertragungswege und die für die Selektion der nachrichtendienstlich relevanten Kommunikationsinhalte benutzten **Suchbegriffe** („Telekommunikationsmerkmale“/„Selektoren“) **ausnahmslos mit dem gesetzlichen Auftrag des BND vereinbar** sind. Dies muss insbesondere für Suchbegriffe gelten, die eventuell aufgrund einer Kooperation mit ausländischen Stellen eingesteuert werden. Hier muss sichergestellt werden, dass diese mit besonderer Sorgfalt auf einen **möglichen Verstoß gegen deutsches Recht und deutsche Interessen** überprüft werden.

Hierzu sollte die aufsichtführende Stelle gesetzlich verpflichtet werden, im BND **klare Strukturen mit effektiven internen Prüfmechanismen** vorzusehen, die dies bereits behördenintern gewährleisten können. Ebenso sollte die **Implementierung von Kontroll- und Berichtspflichten gegenüber der aufsichtführenden Stelle** gesetzlich vorgeschrieben werden.

- Telekommunikationsvorgänge, deren Anfangs- und Endpunkt jeweils in **Mitgliedstaaten der Europäischen Union** und in weiteren Ländern liegt, mit denen entsprechende Abkommen geschlossen sind, sollten gesetzlich besonders geschützt werden. EU-Bürger sollten grundsätzlich von einer Informationserhebung ausgeschlossen sein. Ausnahmen können gelten, wenn einer der in § 5 G10 genannten besonderen Gefahrenbereiche betroffen ist. Denn in solchen Fällen dürfte auch in das Fernmeldegeheimnis deutscher Grundrechtsträger eingegriffen werden.
- Eingeführt werden sollte zudem neben einer Verpflichtung zur **Genehmigung durch den Präsidenten des BND bei Erstbeantragung** einer Maßnahme der StraFmA eine **zwingende Evaluation der nachrichtendienstlichen Wirksamkeit** der einzelnen Maßnahmen in regelmäßigen Abständen.
- Das **Verhältnismäßigkeitsprinzip** muss bei der Überwachung von Telekommunikationsverkehren umfassend beachtet und als gesetzliche Voraussetzung festgeschrieben werden:
 - Die Informationen über die Vorgänge im Ausland dürfen nur durch die Fernmeldeaufklärung zu erlangen sein.
 - Von mehreren geeigneten Maßnahmen hat der Bundesnachrichtendienst diejenige zu wählen, die die Betroffenen voraussichtlich am wenigsten beeinträchtigt.
 - Eine Maßnahme darf keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.
- Die Bundesregierung sollte zudem eine gesetzliche Regelung erarbeiten, mit der im Sinne der Verfassungsgerichtsrechtsprechung je nach Übertragungsart (Satellit, Kabel, Richtfunk, Mobilfunk) eine **quantitative Beschränkung** des maximal erfassbaren Routineverkehrs sowohl für paket- als auch für leitungsvermittelte Telekommunikationsverkehre erfolgt. Eine **Totalüberwachung dieses Verkehrs ist auszuschließen** (vgl. BVerfGE 100, S. 313, 377). Zugleich sollte die in § 10 Abs. 4 G10 existierende **20%-Regelung** daraufhin überprüft werden, ob sie angesichts der technologischen Entwicklung noch geeignet ist, den verfassungsgerichtlichen Vorgaben zu genügen.

3.) Zentrale Einbeziehung einer neu strukturierten G10-Kommission

- Wir fordern für sämtliche Maßnahmen der StraFmA des BND eine zentrale Beteiligung einer **grundlegend neu strukturierten und massiv gestärkten G10-Kommission**, die sich an dem bewährten Kontrollmodell bei der strategischen Fernmeldeaufklärung nach § 5 G10 orientiert:

Für sämtliche Maßnahmen der StraFmA des BND sollte - nach Ablauf einer Übergangsphase - eine **vorherige Genehmigung durch die G10-Kommission** erforderlich sein.

Bei der Antragstellung sind aber **Differenzierungen** zwischen Maßnahmen im Bereich von G10-Verkehr (StraFmA-G10) und der StraFmA von Routineverkehr (StraFmA-R) durchaus vorstellbar, weil sich die aus Art. 10 GG abzuleitenden objektiv-rechtlichen Schutzpflichten unterscheiden von der abwehrrechtlichen Dimension des Grundrechtsschutzes (vgl. etwa: BVerfGE 100, S. 313, 362; 125, S. 39, 78) und auch die entsprechenden völkerrechtlichen Regelungen ein erheblich niedrigeres Schutzniveau gegenüber dem des Grundgesetzes aufweisen. Zugleich sind die Aufgaben des BND und die Bedingungen ihrer Erfüllung außerhalb des G10 anders zu gewichten. Dabei ist zudem immer zu berücksichtigen, dass die **Wahrnehmung des Verfassungsauftrags der Nachrichtendienste nicht gefährdet werden darf** (vgl. nur: BVerfGE 31, S. 58, 72; 57, S. 250, 284; 92, S. 26, 41; 100, S. 313, 363; 122, S. 120, 141).

Diese notwendigen Differenzierungen dürften vor allem in einem **längeren Bearbeitungszeitraum** sowie in einem **flexibleren Umgang mit den eingesetzten Suchbegriffen** liegen. Eine Vorab-Vorlage und -Genehmigung sämtlicher eingesetzter Selektoren durch die Kommission wie dies in § 10 Abs. 4 G10 für die G10-Verkehre verlangt wird, dürfte im Bereich des Routineverkehrs weder praktikabel noch aufgrund der eingeschränkten Wirkung von Artikel 10 GG in diesem Bereich erforderlich sein. Hier dürfte eine **intensive und kontinuierliche begleitende breite Stichprobenkontrolle** durch die Kommission bzw. ihre Mitarbeiter ausreichen.

- Die grundsätzliche Genehmigung einer entsprechenden Maßnahme der StraFmA-R sollte trotzdem grundsätzlich **im Vorhinein** erteilt werden müssen. Im **schriftlichen Antrag** dürften zumindest folgende Angaben erforderlich sein:
 - Art, Dauer und Umfang der Erfassung sowie eine ausführliche schriftliche Begründung ihrer Notwendigkeit
 - Bezug zum Auftragsprofil der Bundesregierung für den BND (APB)
 - Betroffenes Gebiet
 - Zahl und Qualität der betroffenen Übertragungswege, die erfasst werden sollen, einschließlich Darlegung einer quantitativen Begrenzung des Zugriffs auf einen bestimmten Übertragungsweg zur Verhinderung einer Totalerfassung
 - Darlegung, warum die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre

- Angaben zur Einhaltung der Beschränkungen der Erhebungsbefugnis und zur Beachtung der Datenschutzvorschriften, insbesondere des Filtersystems, der Art der verwendeten Selektoren und der Lösungsstufen sowie beabsichtigter Übermittlungen von Daten an dritte Stellen
- Angaben zur Beteiligung des G10-Juristen im BND und des BND-Präsidenten bei Erstbeantragung
- Die Genehmigung soll die Erfassung nur erlauben, soweit sie explizit beantragt worden ist. Sie darf nicht als „Türöffner“ benutzt werden, um weitere Verkehre zu erfassen, die nicht Gegenstand des Antrags sind. Die Genehmigung einer Maßnahme der StraFmA-R soll dann **gegenüber Dritten im Inland** (Providern, Netzbetreibern etc.) die gleiche Wirkung haben wie eine G10-Anordnung.
- Ist mit der Erfassung kabelgebundener Verkehre im Inland die Erfassung von Verkehren nach § 5 G10 **nicht beabsichtigt**, ist durch gesetzliche Vorgaben sicherzustellen, dass eine möglichst frühe und effektive Filterung und **Löschung von G10-Daten** durch entsprechende technische Maßnahmen nach dem jeweiligen **Stand der Technik** erfolgt.
- Die **G10-Kommission** muss jederzeit berechtigt sein, sämtliche **Suchbegriffe**, die zur Selektion auf die erhobenen Informationen Anwendung finden, beim BND **ein-zusehen und zu prüfen**, ob sie der Aufgabenerfüllung dienen und nicht gegen deutsche Interessen verstoßen. Gleiches gilt für alle eingesetzten Filter, deren Wirkungsweise und Parameter. Sämtliche **Rechte aus § 15 Abs. 5 G10** sind auf die Kontrolle der gesamten StraFmA des BND zu erstrecken.
- Gleiches gilt für die Überprüfung von Daten, die **an ausländische Stellen übermittelt** werden sowie für die allgemeine Verarbeitung und Nutzung der gewonnenen Daten im BND.
- Die **Zusammensetzung** der G10-Kommission sollte den neuen umfangreichen Zuständigkeiten angepasst werden. An die **Erhöhung der Zahl der Mitglieder** ist zu denken.

Dabei wäre es wünschenswert, dass nicht nur der Vorsitzende der G10-Kommission die **Befähigung zum Richteramt** aufweisen muss (vgl. § 15 Abs. 1 G10), sondern **in ausreichendem Maße juristischer Sachverstand** in der Kommission sichergestellt ist. Dem anderweitig vorgebrachten Vorschlag, teilweise hauptamtliche Mitglieder der G10-Kommission vorzusehen, dürfte allerdings entgegenstehen, dass es nicht Mitglieder „erster und zweiter Klasse“ geben soll.

- Es sollte gesetzlich vorgesehen werden, dass nach Möglichkeit **keine aktiven oder ehemaligen Abgeordneten** in die G10-Kommission entsandt werden.
- Der bislang monatliche **Tagungsrhythmus der G10-Kommission** (§ 15 Abs. 4 G10) muss **erhöht** werden. Es ist auch eine neue Arbeitsaufteilung innerhalb der G10-Kommission durch Implementierung eines **Berichterstatterwesens** vorstellbar.
- Die G10-Kommission sollte zudem - ähnlich wie das Parlamentarische Kontrollgremium in § 7 PKGrG - gesetzlich die Möglichkeit erhalten, zu besonderen Themen, vor allem zu technischen Fragestellungen, **Sachverständige zu beauftragen**.

- Die G10-Kommission ist darüber hinaus mit **Personal- und Sachmitteln** so auszustatten, dass sie ihre Kontrollaufgaben effizient, regelmäßig und umfassend wahrnehmen kann. Ihr Unterstützungspersonal muss professionellen juristischen, technischen und nachrichtendienstlichen Sachverstand bereitstellen. Die gesetzlichen Vorgaben hierfür müssen **erheblich konkreter** ausgestaltet werden als sie es bislang in § 15 Abs. 3 G10 sind.
- Sämtliche **Rechte** der Mitglieder der G10-Kommission sollten durch diese auch **auf ihre Mitarbeiterinnen und Mitarbeiter übertragen** werden können.
- Die G10-Kommission sollte gesetzlich verpflichtet werden, aus ihrem Unterstützungspersonal einen **hauptamtlichen Datenschutzbeauftragten** zu bestellen, der die **Einhaltung aller Vorschriften** über den Datenschutz sowie der Erhebung, Verarbeitung und Nutzung der Daten aus der nachrichtendienstlichen Fernmeldeaufklärung verantwortlich überwacht. Dieser sollte in **engem Austausch mit der Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI)** stehen.

Ihm ist - ebenso wie anderen beauftragten Mitarbeiterinnen und Mitarbeitern der Kommission - **Auskunft** zu seinen Fragen sowie **Einsicht** in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme sowie jederzeit **Zutritt** in alle Diensträume zu gewähren. Die gesetzlichen Zuständigkeiten und Kompetenzen der BfDI bleiben davon unberührt.

- Es sollten im Rahmen der gesetzlichen Neuregelung **umfangreichere Berichtspflichten der G10-Kommission** gegenüber dem Parlamentarischen Kontrollgremium vorgesehen werden, um auf diesem Gebiet unter Beachtung der Geheimenschutzbelange **Transparenz so weit als irgend möglich herzustellen**.
- Schließlich sollte allgemein eine **bessere Verzahnung der verschiedenen Kontrollinstanzen** in diesem Bereich (G10-Kommission, Parlamentarisches Kontrollgremium [PKGr], Vertrauensgremium nach § 10a Abs. 2 der Bundeshaushaltsordnung und Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [BfDI]) gesetzlich ermöglicht werden.
- Den in anderen Zusammenhängen vorgebrachten Vorschlag eines vom gesamten Parlament mit Mehrheit zu wählenden und öffentlich agierenden „**Geheimdienstbeauftragten**“ **lehnen wir ab**, weil damit die Oppositionsrechte im PKGr beschnitten würden und die Gefahr entsteht, dass aktuelle nachrichtendienstliche Missstände einfach öffentlich „abmoderiert“ werden könnten. Vor allem darf nicht der Eindruck entstehen, dass sich das Parlament ureigenster Aufgaben durch Delegation entledigt. **Die Herrschaft über die Kontrolltätigkeit muss beim Parlament selbst und beim PKGr mit seinen austarierten Minderheitsrechten verbleiben!**

Es kann jedoch durchaus daran gedacht werden, eine **eigene Arbeitseinheit** in der Bundestagsverwaltung **mit mehreren Referaten** - entsprechend der Unterstützungsstruktur beim Wehrbeauftragten - für den gesamten Bereich der Kontrolle der Nachrichtendienste, einschließlich der Unterstützung der G10-Kommission, vorzusehen.

4.) Datenschutz umfassend gewährleisten!

- Wir fordern, dass der Datenschutz bei der Erhebung, Speicherung und Verarbeitung der gewonnenen Daten aus der StraFmA-R lückenlos zu beachten ist. Die bereits bestehenden **Datenschutzbestimmungen** müssen unbeschränkt auch auf den Routineverkehr Anwendung finden. Regierungsinterne „Weltraumtheorien“ oder Theorien vom „virtuellen Ausland“ dürfen keinen Bestand mehr haben.
- Bei automatisierter Datenverarbeitung muss durch gesetzliche Klarstellung die Beachtung des jeweiligen **Standes der Technik** sichergestellt werden. Eine Ausfilterung mit spurloser **Löschung** hat automatisiert möglichst früh und ohne Möglichkeit der Kenntnisnahme zu erfolgen. Ist dies in Einzelfällen technikbedingt nicht möglich, muss es spätestens auf der ersten manuellen Filter- oder Verarbeitungsebene geschehen.
- Die Neuregelung soll vorsehen, dass die **Übermittlung** personenbezogener Daten aus der StraFmA-R an **ausländische öffentliche Stellen** nur zulässig ist, wenn die Übermittlung zur Erfüllung der Aufgaben des BND oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist (§ 9 BNDG i.V.m. § 19 Abs. 3 BVerfSchG). Die Übermittlung an einen ausländischen Partnerdienst **müsste** also **unterbleiben**, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende **schutzwürdige Interessen** des Betroffenen entgegenstehen.

Dies wäre vor allem auch der Fall, wenn tatsächliche Anhaltspunkte bestünden, mit der Übermittlung würden nationale Restriktionen des Partnerdienstes umgangen werden („**Ringtausch**“). Dies ist mittels einer geeigneten gesetzlichen Bestimmung zu untersagen.

- Es sollte auch geprüft werden, ob und inwieweit eine Normierung der **Übermittlung nicht personenbezogener Daten**, insbesondere an ausländische öffentliche Stellen, erfolgen sollte (vgl. § 14 Abs. 2 BKAG).
- Es ist bei allen Übermittlungen sicherzustellen, dass der Empfänger zwingend immer darauf hingewiesen wird, dass die übermittelten Daten nur zu dem **Zweck** verwendet werden dürfen, zu dem sie ihm übermittelt wurden, und dass sich der BND vorbehält, um Auskunft über die vorgenommene **Verwendung der Daten** zu ersuchen. Die Einhaltung dieser Bedingung muss der BND auch tatsächlich prüfen und die **G10-Kommission** über jede erkannte oder aufgrund konkreter tatsächlicher Anhaltspunkte vermutete unerlaubte Verwendung **unverzüglich unterrichten**.
- Es sollte intensiv geprüft werden, ob es für die **Übermittlung von Metadaten an ausländische öffentliche Stellen** eventuell einer zusätzlichen spezifischen Übermittlungsvorschrift mit weiteren Vorgaben bedarf. Andernfalls sollten jedenfalls die Vorschriften des BNDG für **personenbezogene Daten** (§ 9 BNDG i.V.m. § 19 Abs. 3 BVerfSchG) für anwendbar erklärt werden.
- Zur Wahrung der schutzwürdigen Interessen Betroffener sollte gesetzlich klargestellt werden, dass Übermittlungen von Metadaten aus der StraFmA an ausländische öffentliche Stellen grundsätzlich dann zu unterlassen sind, wenn sie eine genaue **Lokalisierung des Anschlussinhabers** ermöglichen (GPS) und die Gefahr besteht, dass die konkret übermittelten Daten außerhalb des Übermittlungszwecks verwendet werden können (Stichwort: „*Extralegale Tötungen mit bewaffneten Drohnen*“).

Ausnahmen hiervon müssen aber für besondere Einzelfälle (Entführungen im Ausland, konkrete Gefahrenlagen etc.) möglich bleiben. Die G10-Kommission sollte darüber jedoch in jedem dieser Einzelfälle unverzüglich unterrichtet werden.

- Jede Übermittlung von Daten aus der StraFmA ist **aktenkundig** zu machen. Die G10-Kommission ist in regelmäßigen Abständen über den Umfang und die Qualität der Übermittlungen zu **unterrichten**.
- Das **Auskunftsrecht** nach § 7 BNDG sollte auch auf EU-Bürger erstreckt werden. Auf entsprechende Mitteilungspflichten aus § 12 Abs. 2 G10 dürfte im Bereich der StraFmA-R allerdings vollständig verzichtet werden können.
- Zur Gewährleistung der Einhaltung der **gesetzlichen Beschränkungen** der Auslandsüberwachung sollte beim BND jeweils bei der Erfassung, Übermittlung und Löschung von Telekommunikationsdaten ein Mitarbeiter mit Befähigung zum Richteramt beteiligt werden. Seine Beteiligung ist gesetzlich vorzusehen. Diese Aufgabe kann vom bereits bestellten **G10-Juristen** wahrgenommen werden.
- In Anpassung der Rechtslage an die bereits bestehende Praxis sollte unbedingt eine gesetzliche Klarstellung erfolgen, dass die **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)** zur Erfüllung ihrer gesetzlich zugewiesenen Aufgaben gegenüber den Nachrichtendiensten/Sicherheitsbehörden auch personenbezogene Daten verwenden darf, die nach dem G10 erhoben worden sind. Hierzu sollte § 24 Abs. 2 BDSG entsprechend angepasst werden.