

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Stellungnahme

Datum:
18.02.2021

Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur
Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des
Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts
(BT-Drucksache 19/26103)

- 1 Einleitung 2**
- 2 Unzureichende materiellrechtliche Schutzvorschriften 3**
 - 2.1 Mangelhafte Definition journalistischer Vertraulichkeitsbeziehungen 3
 - 2.2 Fehlender Schutz für Verkehrsdaten insb. aus Vertraulichkeitsbeziehungen 4
 - 2.3 Arbiträrer Ausschluss von verhashter und Maschine-zu-Maschine-
Kommunikation von Schutzstandards 5
 - 2.4 Zitiergebot..... 6
- 3 Unzureichende Dokumentation und Kontrollmechanismen 6**
 - 3.1 Fehlende Kontrolle des Einsatzes von Selektoren 6
 - 3.2 Fehlende Kennzeichnung von Daten ermöglicht Umgehung von
Übermittlungsbeschränkungen 7
 - 3.3 Third Party Rule durch die Hintertür? 8
 - 3.4 Der BND bestimmt, was für die Kontrolle erforderlich ist 8
- 4 Ineffiziente Kontrollarchitektur 8**
 - 4.1 Gefahren für die Unabhängigkeit..... 9
 - 4.2 Doppelstrukturen statt Synergien bei der Rechtskontrolle..... 9
 - 4.3 Mangelnde Sanktionsmöglichkeiten 10
 - 4.4 Paralleler Ausbau der parlamentarischen Kontrolle nötig..... 10
- 5 Neue Eingriffsbefugnisse ohne Überwachungsgesamtrechnung..... 11**
- 6 Fazit 11**

1 Einleitung

Die Reform des BND-Gesetzes 2016 war eine Reaktion auf den wohl größten Überwachungsskandal in der Geschichte der Bundesrepublik. Die Enthüllungen des Whistleblowers Edward Snowden hatten offengelegt, dass der BND täglich Millionen von Metadaten erhob und an die NSA weiterleitete. Im Weiteren stellte sich heraus, dass die Datenerhebung auch am deutschen Internetknotenpunkt DE-CIX erfolgte und gar auch gezielt ausländische Angehörige der Presse überwacht worden waren. Diese Tätigkeit entbehrte jeder Rechtsgrundlage und war insbesondere auch den parlamentarischen Kontrollgremien unbekannt.

Eine solche entfesselte Exekutive, dies hat das Bundesverfassungsgericht in seinem Urteil vom 19. Mai 2020 (1 BvR 2835/27, im Weiteren „Urteil“) klargestellt, ist auch gegenüber ausländischen Staatsangehörigen im Ausland mit der durchgehenden Bindung aller Staatsgewalt an die Grundrechte nicht vereinbar, die Art. 1 Abs. 3 GG verlangt. Ihre Grundrechtseingriffe bedürfen der Begrenzung durch angemessene Eingriffsschwellen und, gerade aufgrund der Geheimhaltung gegenüber den Betroffenen, effektiver unabhängiger Kontrolle. Und eine solche Kontrolle ist auf eine angemessene Dokumentation angewiesen.

Die nur partielle und in der Sache halbherzige Kodifizierung der jahrelangen illegalen Abhör-Praxis im Jahr 2016 ist diesen Anforderungen nicht im Ansatz gerecht geworden. Daher hat das Bundesverfassungsgericht sie im Urteil vom Mai 2020 zu Recht aufgehoben. Gleichzeitig hat es der Gesetzgebung umfangreiche Hinweise an die Hand gegeben, welche verfassungsrechtlichen Grenzen eine Neuregelung der – weiterhin grundsätzlich zulässigen – strategische Fernmeldeaufklärung im Ausland zu beachten haben wird. Namentlich hat es ausführlich erläutert, welche Mindestanforderungen sich aus dem Telekommunikationsgeheimnis aus Art. 10 Abs. 1 Satz 2 GG und den Medienfreiheiten aus Art. 5 Abs. 1 Satz 2 GG für eine rechtsstaatliche Einhegung der nachrichtendienstlichen Tätigkeit im Ausland ergeben.

Insbesondere hat es deutlich gemacht, dass **drei Elemente ineinander greifen müssen: Begrenzung der Befugnisse in den Eingriffsgrundlagen, Dokumentation der Eingriffspraxis und eine wirksame Kontrolle.** Die *Begrenzung der Befugnisse* allein ist gerade bei einer im Geheimen operierenden Behörde keine hinreichende Garantie für eine rechtsstaatliche Praxis. Hierfür bedarf es einer *wirksamen Kontrolle*; diese wiederum ist aber auf eine *detaillierte Dokumentation* angewiesen. Fehlt es an einem der drei Elemente, sind die verfassungsrechtlichen Vorgaben nicht erfüllt.

Die erneute Notwendigkeit einer Reform des BND-Gesetzes bietet eine Gelegenheit, die bisherige legislative Praxis zu überdenken. Es ist an der Zeit, grundsätzlich zu reflektieren, welche Rolle Geheimdienste in einer modernen Demokratie spielen können und wie ihre Tätigkeiten mit adäquaten grund- und menschenrechtlichen Standards zu vereinbaren sind. Denn das Urteil des Ersten Senats vom 19. Mai 2020 formuliert nur das absolute grundrechtliche Mindestmaß – das, was in unserem Rechtsstaat gerade noch hinzunehmen ist.

Man kann also rechtspolitisch enttäuscht sein, wenn ein Gesetzgeber sich keine höheren Ziele vornimmt als dieses Mindestmaß abzubilden, statt die bisherigen nachrichtendienstlichen Befugnisse und die Kontrollmechanismen insgesamt in den Blick zu nehmen und einen großen Wurf zu wagen. Der Gesetzesentwurf der Bundesregierung beschränkt sich aber nicht nur auf die im Sicherheitsrecht üblich gewordene „Eins-zu-eins-Umsetzung“ – selbst in der Terminologie (z.B. „gerichtsähnliches Kontrollorgan“, § 40 Abs. 2 BNDG-E). Er reißt teilweise sogar das verfassungsrechtliche Mindestmaß. Überdies fügt er neue Befugnisse hinzu, die aus verfassungsrechtlicher Sicht ebenfalls höchst besorgniserregend sind, ohne dass eine Überwachungsgesamtrechnung ergeben hätte, dass die bisherigen Befugnisse nicht ausreichen.

Aufgrund der Vielzahl von Kritikpunkten, die bereits in verschiedenen Stellungnahmen angeführt worden sind, möchte ich mich im Folgenden insbesondere auf Mängel beim Schutz für besonders

schutzwürdige Vertraulichkeitsbeziehungen und in der Kontrolle beschränken und zur Notwendigkeit einer Überwachungsgesamtrechnung Stellung nehmen.

2 Unzureichende materiellrechtliche Schutzvorschriften

Besorgniserregend ist erstens die Aushöhlung der neu eingeführten Schutzstandards durch Ausnahmen und unkontrollierte Ermessenseinräumung an den BND. Dies betrifft insbesondere den Schutz von Vertraulichkeitsbeziehungen, die im besonderen Fokus des BND-Urteils standen. Hierbei wirkt sich auch der allgemein unzureichende Schutz von sogenannten Metadaten aus.

2.1 Mangelhafte Definition journalistischer Vertraulichkeitsbeziehungen

Das BND-Urteil des Bundesverfassungsgerichts geht zurück auf eine Verfassungsbeschwerde investigativ arbeitender Journalisten und Journalistinnen, die um ihre eigene Sicherheit und die ihrer Quellen fürchteten. Für den Schutz gerade solcher besonders schutzwürdiger Vertraulichkeitsbeziehungen hat das Bundesverfassungsgericht daher explizite, enge Vorgaben gemacht.

So erfordert Art. 5 Abs. 1 Satz 2 GG insbesondere erhöhte Eingriffsschwellen für solche Vertraulichkeitsbeziehungen (vgl. Urteil, Rn. 194, 257). Diese materiellen Anforderungen müssen prozedural durch eine „gerichtsähnliche ex ante-Kontrolle“ abgesichert werden (ebd., Rn. 194), die ggf. ex post nachgeholt werden muss (ebd., Rn. 195). Es ist zwar zu begrüßen, dass § 21 Abs. 2 BNDG-E die Eingriffsschwellen für diese Berufsgruppen gegenüber der früheren Rechtslage deutlich erhöht, wenngleich hier nicht alle Bedenken ausgeräumt sind.¹ Die Schutzwirkung der Norm wird allerdings durch ihre Unbestimmtheit in Frage gestellt.

So fehlt es in § 21 Abs. 1 BNDG-E an einer **Definition des Rechtsbegriffs des „Journalisten“**, der – anders als der des „Geistlichen“ oder des „Rechtsanwalts – gerade nicht an eine institutionelle Zugehörigkeit oder staatliche Zulassung gebunden ist (s.a. Gesetzentwurf S. 76) und daher der Konkretisierung bedarf. Autoritäre Regimes entziehen unliebsamen Reportern und Reporterinnen Akkreditierungen oder sprechen kritischen Medien ihren Status ab.² Zunehmende Bedeutung erlangen demgegenüber sogenannte Bürgerjournalistinnen und -journalisten wie die Gruppe „Raqqah is being slaughtered silently“, die im Schutz der Anonymität die Gräueltaten des IS in Syrien dokumentiert und so einer Weltöffentlichkeit zugänglich macht.³ Die Beschwerdeführer und Beschwerdeführerinnen im BND-Fall, darunter die Trägerin des alternativen Nobelpreises Khadija Ismajilowa, zeigen beispielhaft, welchen Gefahren und Repressionen Journalistinnen und ihre Quellen ausgesetzt sein können und welche zentrale Bedeutung der Schutz der Vertraulichkeit ihrer Arbeit hat.

Dieser Schutz hängt jedoch gemäß § 21 Abs. 1 BNDG-E an der Frage, ob die betreffende Person als „Journalist“ einzuordnen ist. Die Beantwortung dieser zentralen Frage soll allerdings der Behörde selbst überlassen werden. In der Gesetzesbegründung heißt es dazu auf S. 76: „Nähere Vorgaben zur Bewertung durch den Bundesnachrichtendienst sind daher in einer Dienstvorschrift zu regeln, die der Kontrolle durch den Unabhängigen Kontrollrat unterliegt“. Der BND selbst soll also in einer geheimen Dienstvorschrift definieren können, wen er als Journalistin anerkennt. Dies widerspricht nicht nur den Anforderungen des BVerfG an die Normenklarheit und Bestimmtheit der Rechtsgrundlagen seiner geheimen Tätigkeit (Urteil, Rn. 137–139).

¹ Vgl. dazu etwa die Stellungnahme von Reporter ohne Grenzen zum Referentenentwurf, Dez. 2020, S. 6–8.

² Vgl. etwa Reporter ohne Grenzen, Kritik an Lukaschenkos Medienpolitik, 2020, abrufbar unter <https://www.reporter-ohne-grenzen.de/belarus/alle-meldungen/meldung/kritik-an-lukaschenkos-medienpolitik>.

³ <https://www.raqqa-sl.com/en/>.

Für die Anwendung dieser Dienstvorschrift ist auch **keine wirksame Kontrolle vorgesehen**. § 42 Abs. 2 Nr. 3 BNDG-E begrenzt die gerichtsähnliche Kontrolle der Dienstvorschriften auf Vorschriften zur Datenauswertung. Insbesondere fehlt es an einer Dokumentationspflicht für Entscheidungen über die Einordnung konkreter Personen; die in § 42 Abs. 2 Nr. 1 BNDG-E vorgesehene Kontrolle, die nur die Verwendung der Daten nach § 21 Abs. 3 BNDG-E erfasst, wird dadurch ausgehöhlt. Auf höchst ärgerliche Weise irreführend ist dabei der Hinweis in der Gesetzesbegründung, § 23 Abs. 7 BNDG-E stelle eine wirksame Kontrolle der Suchbegriffe durch den UKr sicher;⁴ § 23 Abs. 6 BNDG-E, auf den sich diese Norm bezieht, schließt jedoch in Satz 3 die Erforderlichkeit der Nennung der Suchbegriffe in der vom UKr zu kontrollierenden Anordnung gerade aus (s. dazu unten 3.1).

Zu begrüßen ist, dass der Gesetzentwurf nicht mehr nahelegt, dass der BND bei der Einordnung auf inhaltliche Kriterien abstellen könnte. So ist in der Gesetzesbegründung nur mehr von der Abgrenzung von „als Journalisten getarnten Vertreterinnen oder Vertreter fremder Nachrichtendienste“ die Rede (Gesetzentwurf, S. 76) und nicht mehr von „Propaganda“. Dies wäre auch verfassungswidrig. Denn der Schutz der Medienfreiheiten aus Art. 5 Abs. 1 Satz 2 GG verlangt strikte Inhaltsneutralität, solange keine allgemeinen Gesetze verletzt werden.⁵ Zu Recht stellt das Bundesverfassungsgericht daher auf Personen ab, deren Tätigkeiten „durch Freiheit und Unabhängigkeit gekennzeichnet sind“ (Urteil, Rn. 196).

Um solchen Praxen vorzubeugen und die verfassungsrechtlichen Anforderungen an Normenklarheit und Bestimmtheit zu erfüllen, **sollte das Gesetz selbst Kriterien für die Einordnung von Journalisten und Journalistinnen vorsehen** und dabei auf die Arbeitsweise abstellen. Die Gesetzesbegründung sollte **auf entsprechende journalistische Standards für vertrauenswürdige Medienarbeit verweisen**, wie sie beispielsweise durch das EU-geförderte Pilotprojekt der „Journalism Trust Initiative“ erarbeitet worden sind.⁶ Um die verfassungsrechtlich erforderliche wirksame Kontrolle zu ermöglichen, ist zudem eine **Dokumentation der Entscheidung über die Schutzwürdigkeit** vorzuschreiben.

2.2 Fehlender Schutz für Verkehrsdaten insb. aus Vertraulichkeitsbeziehungen

Während § 19 BNDG-E nur personenbezogene Inhaltsdaten erfasst, regelt § 26 BNDG-E die Verarbeitung personenbezogener Verkehrsdaten. Die Gesetzesbegründung zu § 26 BNDG-E geht davon aus, letztere greife „mangels unmittelbaren Bezugs zu einer Telekommunikation im Sinne des Artikel 10 GG lediglich in das Recht auf informationelle Selbstbestimmung des Betroffenen ein“ (Gesetzentwurf, S. 85). Entsprechend sieht § 26 Abs. 3 BNDG-E Ausnahmen nur für Deutsche, inländische juristische Personen und im Bundesgebiet aufhältige Personen (G10-Verkehre) vor, nicht für besonders schutzwürdige Vertraulichkeitsbeziehungen i.S.d. § 21 Abs. 1 BNDG-E. Die Verarbeitung von Metadaten im Übrigen wird überhaupt nicht geregelt.⁷

⁴ „§ 23 Absatz 7 sieht zudem vor, dass der Unabhängige Kontrollrat die Rechtmäßigkeit der Anordnungen der Suchbegriffe vor deren Verwendung prüft. Damit wird der verfassungsrechtlichen Vorgabe, den Schutz von Vertraulichkeitsbeziehungen durch eine gerichtsähnliche ex ante-Kontrolle abzusichern, umfassend Rechnung getragen.“ S. 77 des Gesetzentwurfs.

⁵ BVerfGE 124, 300, Rn. 54 – *Wunsiedel*.

⁶ CEN Workshop Agreement CWA 17493, December 2019, ICS01.140.40, <ftp://ftp.cencenelec.eu/EN/News/WS/2019/JTI/CWA17493.pdf>.

⁷ Hierzu erläutert der Gesetzentwurf, S. 62: „Metadaten sind alle über die Inhaltsdaten hinausgehenden Daten. Dies sind zum Beispiel technische und fernmeldebetriebliche Informationen, die die Umstände einer Telekommunikation, den technischen Übertragungsweg oder auch die Bereitstellung der technischen Mittel einer Übertragung ohne willentliches Zutun des Nutzers beschreiben. Als Metadaten werden beispielsweise Daten bezeichnet, die den Aufbau und die Benutzung anderer Daten beschreiben, oder Daten über Daten, wie Datentyp, Bedeutung, Beziehungen zwischen Entitätstypen, Integritätsbedingungen, Verdichtungsregeln.“

Damit verkennt der Gesetzentwurf die Reichweite von Art. 5 Abs. 1 Satz 2 GG. Die Medienfreiheiten schützen die journalistische Tätigkeit umfassend „von der Beschaffung der Information bis zur Verbreitung“.⁸ Daher sind auch reine Sachdaten (Metadaten) vom Schutz des Art. 5 Abs. 1 Satz 2 GG umfasst.

Insbesondere **Verkehrsdaten lassen potentiell gefährliche Rückschlüsse auf besonders schutzwürdige Vertraulichkeitsbeziehungen zu**. Der Gesetzentwurf definiert sie als „solche Metadaten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (vgl. § 3 Nummer 30 TKG).“ Die Legaldefinition in § 3 Nr. 30 TKG liest sich deutlich aufschlussreicher: Zu den Verkehrsdaten gehören nämlich beispielsweise die Nummer und Kennung der an der Kommunikation beteiligten Anschlüsse, personenbezogene Berechtigungskennungen, eventuelle Standortdaten bei der Nutzung eines Handys, Datum und Uhrzeit des Beginns und Endes der Kommunikation (Zeitstempel) und die übermittelten Datenmengen. Hiermit lassen sich problemlos beispielsweise gefährdete journalistische Quellen identifizieren. Auch E-Mail-Betreffzeilen gehören zu den nicht hinreichend geschützten Verkehrsdaten; diese können sogar Rückschlüsse auf den Inhalt der Kommunikation zulassen und fallen damit in den Kernbereich von Vertraulichkeitsbeziehungen. Die Identifizierbarkeit von Personen erkennen auch § 26 Abs. 3 Satz 2 Nr. 2 und Satz 3 BNDG-E an, die für deutsche und inländische Personen eine Unkenntlichmachung der Daten erfordern. Eine entsprechende Regelung für Personen i.S.d. § 21 Abs. 1 BNDG-E fehlt. Dies ist mit Art. 5 Abs. 1 Satz 2 GG nicht vereinbar. Der Gesetzentwurf verkennt zudem, dass der Schutz von Art. 10 Abs. 1 GG auch die Kommunikationsumstände (ob, wann, wer, wie oft) umfasst, die sich aus den Verkehrsdaten ergeben.⁹ Gerade die massenhafte Erhebung lässt weitreichende Rückschlüsse auf das Kommunikationsverhalten zu. Die generelle Ausschluss von Verkehrsdaten vom Schutz ist daher mit dem Fernmeldegeheimnis nicht vereinbar.

Auch die in § 33 BNDG-E vorgesehene automatisierte Übermittlung von unselektierten personenbezogenen Verkehrsdaten erlaubt aus den genannten Gründen die Erstellung von Profilen über Medienschaffende und ihre Quellen. Hier fehlt eine Schutzvorschrift entsprechend § 32 Abs. 4 Nr. 3 und Abs. 5 BNDG-E.

Hier muss dringend nachgebessert werden. **Der Gesetzgeber sollte die Trennung zwischen personenbezogenen Inhalts- und Verkehrsdaten aufgeben** und einen umfassenden Schutz sicherstellen; als Vorbild kann das niederländische Recht dienen. **Zumindest müssen § 26 und § 33 BNDG-E um einen wirksamen Schutz von Vertraulichkeitsbeziehungen i.S.d. § 21 Abs. 1 BNDG-E erweitert werden**. Hiervon müssen sowohl die primär geschützten Personen (z.B. Journalisten) als auch ihre vom Schutz der Vertraulichkeitsbeziehung mit umfassten Kontaktpersonen erfasst werden.

2.3 Arbiträrer Ausschluss von verhashter und Maschine-zu-Maschine-Kommunikation von Schutzstandards

Auch der in § 26 Abs. 3 Satz 1 BNDG-E bei der Verarbeitung von personenbezogenen Verkehrsdaten vorgesehene Schutz deutscher Staatsangehöriger, inländischer juristischer Personen oder im Bundesgebiet aufenthältiger Personen (G10-Verkehre) wird auf unverhältnismäßige Weise ausgehöhlt und umgangen, indem § 26 Abs. 3 Satz 2 BNDG-E Ausnahmen vom Verarbeitungsverbot für „Maschine-zu-Maschine-Kommunikation“ sowie für rudimentär „unkenntlich“ gemachte Daten wie Hashes von Telefonnummern vorsieht.

Beim Hashing wird aus einem vorgegebenen Wert mit variabler Länge – beispielsweise einer Telefonnummer – eine Zeichenkette mit einer festen Länge gebildet. Dabei wird derselbe Wert immer durch dieselbe Zeichenkette repräsentiert; es handelt sich insofern um eine Pseudonymisierung.

⁸ BVerfGE 20, 162, 176 – *Spiegel*.

⁹ BVerfGE 107, 299 (319 f.); 113, 348 (383); 115, 166 (183); 100, 313 (359).

In Kombination mit Aufenthaltsorten und Zeitstempeln – für die der Gesetzentwurf keine Unkenntlichmachung vorsieht (Gesetzentwurf, S. 86) – **können hieraus daher durchaus Rückschlüsse auf die beteiligten Personen gezogen werden.** In diesem Fall unterfallen die Daten weiterhin dem Schutz des Art. 10 GG, weswegen die unqualifizierte Ausnahme nicht mit dem Grundgesetz vereinbar ist. Besonders besorgniserregend ist dies für Journalistinnen und Journalisten, deren Quellen auf diese Weise identifizierbar bleiben (s.o.).

Aber auch aus der „Maschine-zu-Maschine-Kommunikation“ zwischen zwei maschinellen Endpunkten können persönlichkeitsrechtsrelevante Informationen gezogen werden. Aus der sensorischen Übertragung, wie viel Strom, Gas oder Datenvolumen eine Person zu einem bestimmten Zeitpunkt verbraucht hat, können zum Beispiel **Rückschlüsse auf ihren Lebenswandel** gezogen werden. Auch Daten von Fitness-Trackern, Banküberweisungen oder Ortungsdaten fallen in diese Kategorie; letzteres lässt beispielsweise Rückschlüsse auf die Teilnahme an Versammlungen zu. Von der Ausnahme erfasst ist aber auch die Nutzung digitaler Anonymisierungswerkzeuge wie beispielsweise anonymer Briefkästen oder des Tor-Netzwerk. Solche Werkzeuge spielen in der internationalen journalistischen Arbeit, die insbesondere bei Investigativrecherchen in Medienverbänden inzwischen eine zentrale Rolle spielen. Die **Nutzung dieser technischen Mittel zum Schutz von Quellen und Inhalten darf gerade nicht zur Aushöhlung des Schutzes vor nachrichtendienstlicher Überwachung führen.**

Insofern **verkennt der Gesetzentwurf nicht nur die Reichweite des Art. 10 GG**, wenn in der Begründung angenommen wird, die „bloße Maschine-zu-Maschinekommunikation“ unterfalle nicht dem Schutz des Fernmeldegeheimnisses (Gesetzentwurf, S. 86). **Er verkennet auch die bereits ausgeführte umfassende Schutzwirkung des Art. 5 Abs. 1 Satz 2 GG.**

2.4 Zitiergebot

Irritierend ist angesichts des BND-Urteils, das gerade die Verletzung des Zitiergebots aus Art. 19 Abs. 2 GG gerügt hat, dass § 68 BNDG-E nur eine Beschränkung von Art. 10 und 13 GG nennt, während **Art. 5 Abs. 1 Satz 2 GG fehlt**, obwohl § 21 Abs. 2 und 3 BNDG-E explizit Eingriffe in die Vertraulichkeitsbeziehungen auch der Presse zulassen.

3 Unzureichende Dokumentation und Kontrollmechanismen

Die vielfache Erhöhung des grundrechtlichen Schutzniveaus im Entwurf der Bundesregierung ist begrüßenswert; allerdings werden die grundrechtlichen Mindestanforderungen teilweise immer noch unterschritten. Zudem genügen, wie das Bundesverfassungsgericht klargestellt hat, auch eng gefasste Ermächtigungsnormen noch nicht; es bedarf gerade aufgrund der Geheimhaltung der Praxis der Behörde auch einer durchgehend wirksamen Kontrolle, die ihrerseits auf eine umfassende Dokumentation angewiesen ist. Im Entwurf der Bundesregierung wird **die Effektivität der Kontrollmechanismen vielfach noch durch verfahrensrechtliche Intransparenz und mangelnde Dokumentationspflichten ausgehöhlt.**

3.1 Fehlende Kontrolle des Einsatzes von Selektoren

Die Kontrollierbarkeit der vom BND verwendeten Suchbegriffe (Selektoren) war einer der zentralen Punkte des Urteils des Bundesverfassungsgerichts. Das Gericht betonte das besondere Eingriffsgewicht der gezielt personenbezogenen Überwachungen durch Einsatz formaler Suchbegriffe wie Telekommunikationskennungen: „Die strategische Fernmeldeaufklärung erhält dadurch eine grundlegend weiterreichende Eingriffstiefe und rückt näher an die individuelle Telekommunikationsüberwachung heran“ (Urteil, Rn. 152; s.a. Rn. 185). Notwendig sei daher in Bezug auf den Einsatz von Selektoren eine Begrenzung der möglichen Gründe und Gesichtspunkte für eine gezielte strategische Überwachung und besondere Schutzmechanismen, einschließlich einer

gerichtsähnlichen Ex-ante-Kontrolle, für Maßnahmen gegenüber möglichen Verursachern von Gefahren oder Adressaten möglicher Folgemaßnahmen (Urteil, Rn. 187 f.).

Die **Kontrollierbarkeit von „Verfahrensregelungen, [...] die die Ausrichtung auf die jeweiligen Zwecke rationalisierend strukturieren“** (Urteil, Rn. 178) gehört zu den Kernanforderungen, die das Gericht aus den Grundrechten ableitet. Diese Anforderungen setzt der Regierungsentwurf deutlich unzureichend um.

So normieren § 23 Abs. 4 und 7 BNDG-E zwar die Rechtskontrolle von Anordnungen für strategische Aufklärungsmaßnahmen nach §§ 19 und 20 BNDG-E durch den Unabhängigen Kontrollrat. § 23 Abs. 2, 3 und 6 BNDG-E enthalten auch detaillierte Anforderungen zum Inhalt der Anordnung solcher Maßnahmen. **Es fehlt jedoch eine Vorschrift, nach der dem UKr auch die Suchbegriffe mit entsprechender Begründung vorgelegt werden müssten.** Daher ist unklar, wie eine Rechtskontrolle der Suchbegriffe durch den UKr durchgeführt werden soll. Für gezielte Maßnahmen nach § 19 Abs. 5 BNDG-E fehlt jede Erwähnung. Für die gezielte Erhebung personenbezogener Daten nach § 20 Abs. 1 und 2 und § 21 BNDG-E (von EU-Einrichtungen, mitgliedstaatlichen Stellen oder Unionsangehörigen oder von vermuteten Verursachern von Gefahren und aus Vertraulichkeitsbeziehungen) erklärt § 23 Abs. 6 S. 3 BNDG-E sogar die Nennung einzelner Suchbegriffe in der Anordnung explizit für *nicht* erforderlich. Das Verbot der gezielten Erhebung von personenbezogenen Daten zum Zwecke der Erlangung von Daten aus einer Vertraulichkeitsbeziehung aus § 21 Abs. 1 BNDG-E unterliegt damit keiner wirksamen Kontrolle. Dies ist mit den klaren Anforderungen des Bundesverfassungsgerichts nicht vereinbar.

Soweit ersichtlich, **fehlt es auch an einer gerichtsähnlichen Vorabkontrolle für die Weitergabe von personenbezogenen Daten an ausländische Geheimdienste**, die mithilfe von Selektoren erhoben wurden, die jene benannt haben. Das Bundesverfassungsgericht hat für die automatisierte Übermittlung an den jeweiligen ausländischen Dienst eine gegebenenfalls händische Prüfung gefordert, ob Daten „Personen zuzuordnen sind, deren Kommunikation auch zur Vermeidung staatlicher Repressionen besondere Vertraulichkeit verlangt“, sowie für Einzelfallentscheidungen eine gerichtsähnliche Vorabkontrolle (Urteil, Rn. 257). In § 32 BNDG-E findet sich dieser Kontrollmechanismus nicht wieder; insbesondere nennt § 32 Abs. 1 Satz 3 BNDG-E nicht § 23 BNDG-E, der die Anordnung und Kontrolle von strategischen Überwachungsmaßnahmen regelt. Auch in § 42 Abs. 1 BNDG-E fehlen die §§ 30 ff. BNDG-E als Gegenstände der gerichtsähnlichen Vorabkontrolle.

3.2 Fehlende Kennzeichnung von Daten ermöglicht Umgehung von Übermittlungsbeschränkungen

Gemäß § 19 Abs. 10 BNDG-E muss der BND personenbezogene Daten bei der Übermittlung als aus der strategischen Fernmeldeaufklärung gem. § 19 Abs. 1 BNDG-E stammend kennzeichnen, noch danach, mit welchen Mitteln sie erhoben wurden. Nachvollziehbar ist allenfalls die Sorge, dass dies ausländischen Nachrichtendiensten Rückschlüsse auf die technische Leistungsfähigkeit des BND ermöglichen würde (so der Gesetzentwurf, S. 74). Für die Inlandsübermittlung ist nicht ersichtlich, welchen legitimen Zweck diese Ausnahme verfolgen soll.

Damit droht jedoch eine **Umgehung der Anforderungen an die Übermittlung** solcher Daten an andere Stellen, die das Bundesverfassungsgericht fein ausdifferenzierten formuliert hat (Urteil, Rn. 211ff.). Denn ohne Kennzeichnung kann der Inlandsgeheimdienst, an den die Daten weitergeleitet wurden, nicht mehr nachvollziehen, dass diese besonderen Übermittlungsbeschränkungen unterliegen. Damit gehen die insoweit geltende Unterrichtungspflicht aus § 29 Abs. 12 Satz 1 BNDG-E und der Zweckbindungsgrundsatz des § 29 Abs. 12 Satz 2 BNDG-E ins Leere.

Das verunmöglicht auch eine wirksame Kontrolle, für die die Kennzeichnung zentrale Voraussetzung ist. Dies ist mit Art. 10 Abs. 1 GG unvereinbar.

3.3 Third Party Rule durch die Hintertür?

Das Bundesverfassungsgericht hat klargestellt, dass die sogenannte „third party rule“ eine effektive Kontrolle des BND nicht behindern darf (Urteil, Rn. 292 ff.). Bei dieser „Regel“ handelt es sich um eine Vereinbarung zwischen Nachrichtendiensten, dass die einander übermittelten Daten keiner „third party“ überlassen werden dürfen. Schwierigkeiten erzeugt dies insbesondere für die parlamentarische Kontrolle, wie der Zweite Senat 2016 bekräftigt hat.¹⁰ Der Erste Senat hat allerdings im BND-Urteil klargestellt, dass diese Regel nicht auch der Rechtskontrolle im Wege stehen darf, die umso wichtiger ist, als es hier an parlamentarischen Kontrollmöglichkeiten mangelt.

§ 55 Abs. 2 S. 1 BNDG-E sieht vor, dass die Unterrichtungspflicht des BND gegenüber dem Unabhängigen Kontrollgremium sich nur auf Informationen und Gegenstände erstreckt „die der Verfügungsberechtigung des Bundesnachrichtendienstes unterliegen“. Dazu heißt es auf S. 130 der Gesetzesbegründung: „Diese Regelung trägt dem Umstand Rechnung, dass die Kontrolle des Unabhängigen Kontrollrates an die [sic] für die nachrichtendienstlichen Zusammenarbeit essenzielle Third Party Rule nicht Halt macht.“ Tatsächlich droht allerdings eine Wiedereinführung der „third party rule“ die Hintertür:

Die grundrechtlich gebotene umfängliche Kontrolle setzt voraus, dass die „third party rule“ den der Geheimhaltung verpflichteten, unabhängigen Kontrollinstanzen, die nicht in das Parlament und dessen politische Kommunikationszusammenhänge eingebunden sind, nicht entgegenhalten werden kann (Urteil, Rn. 292, 294). Hierfür macht der Gesetzentwurf aber keine Vorgaben. Eine diesbezügliche Vorabkontrolle der Absichtserklärungen durch das UKr ist in §§ 31, 42 BNDG-E nicht vorgesehen, eine nachträgliche Kontrolle könnte bestehende Bindungen möglicherweise nicht mehr wirksam beseitigen. Dies ist mit dem Grundgesetz in der Auslegung durch das BVerfG nicht vereinbar.

Zudem hat der BND zwar bei mit ausländischen Nachrichtendiensten gemeinsam genutzten Orten oder Dateien dem UKr die Kontrolle über seinen Teil der Daten und Maßnahmen (die seiner „alleinigen Verfügungsberechtigung“ unterliegen, § 56 Abs. 3 Satz 1 BNDG-E) zu ermöglichen. Die Ausgestaltung dieser Kontrolle, insbesondere eine Einsicht in die informationstechnischen Systeme selber (statt nur in Kopien) und die erforderliche Ausstattung gegebenenfalls notwendiger Sonderbereiche für die Einsichten ist in § 56 Abs. 3 Satz 2 BNDG-E nicht ausreichend klar geregelt. Hier **droht die Effektivität der Kontrolle in der Praxis ausgehöhlt zu werden**. Zumindest die Klarstellungen auf S. 130 der Gesetzesbegründung sollten in die Norm selbst aufgenommen werden.

3.4 Der BND bestimmt, was für die Kontrolle erforderlich ist

Ähnlich besorgniserregend ist, dass der BND dem UKr Zutritt und Zugang nur insoweit einräumen muss, als „dies für die Durchführung der Kontrolle erforderlich ist“. Was erforderlich ist, bestimmt der BND selbst; diese Entscheidung unterliegt keinerlei Kontrolle. Hierdurch wird die **Wirksamkeit der Kontrolle in verfassungsrechtlich höchst bedenklichem Maße beschränkt**.

4 Ineffiziente Kontrollarchitektur

Einer der Hauptpunkte des Urteils war es, dass es einer ausgebauten unabhängigen objektivrechtlichen Kontrolle der Tätigkeiten des BND bedarf (Urteil, Rn. 267ff.). Der Gesetzesentwurf der Bundesregierung entwirft eine **hoch diffuse und ineffiziente Kontrollarchitektur**, der es an vielen Stellen an der notwendigen Unabhängigkeit fehlt. Sie wird den Anforderungen des Urteils daher nicht gerecht.

¹⁰ Dazu BVerfG, Beschluss v. 13. Oktober 2016 – 2 BvE 2/15 – *Selektorenliste*. Dazu auch im BND-Urteil Rn. 294.

4.1 Gefahren für die Unabhängigkeit

Zunächst ist besorgniserregend, dass Unabhängiger Kontrollrat (UKr) eng an das Bundeskanzleramt gebunden ist, dem der zu kontrollierende BND nachgeordnet ist:

Gemäß § 57 Abs. 2 S. 1 BNDG-E darf der UKr dem Bundeskanzleramt (BKAm) die Personalverwaltung und Personalwirtschaft übertragen. Der enge Zeitplan für den Aufbau dieser Stelle lässt befürchten, dass dem unabhängigen Kontrollrat keine andere Wahl bleibt, als dieses Angebot anzunehmen. Gemäß § 41 Abs. 5 und § 55 Abs. 2 BNDG-E ist das BKAm vor Erlass einer Geschäftsordnung/Verfahrensordnung des UKr und vor Veröffentlichung einer abstrakten Unterrichtung des Bundestages anzuhören. Gemäß § 43 Abs. 3 Satz 3 BNDG-E werden die Vorschläge des BGH und der Bundesanwaltschaft für die Mitglieder des gerichtsähnlichen Kontrollorgans der Bundesregierung vor der Wahl durch das PKGr mitgeteilt. Wozu dies notwendig ist, wenn keine Einflussnahme vor der Wahl erfolgen soll, erschließt sich nicht.

Hierdurch wird die Unabhängigkeit der administrativen Kontrolle unnötig in Frage gestellt.

4.2 Doppelstrukturen statt Synergien bei der Rechtskontrolle

Im Sinne der Effizienz der Rechtskontrollen ist schwer nachzuvollziehen, warum die neuen Kontrollmechanismen nicht auf bestehende Strukturen aufgesattelt werden. **Gemeinsame Kontroll-Strukturen für die gesamte Fernmeldeaufklärung könnten Synergien schaffen und effizienter arbeiten.** Insbesondere gilt dies für die dringend notwendige technische Expertise, die nun in mehreren Stellen parallel vorgehalten werden muss, die sich teils überschneidende Kontrollbefugnisse haben. Eine Zerstückelung der administrativen Kontrolle droht auch, das vom Bundesverfassungsgericht ausdrücklich kritisierte Durcheinander an Zuständigkeiten und die oftmals beklagten Wissensasymmetrien zu vertiefen (vgl. Urteil, Rn. 51). Bei Parallelstrukturen ist zudem eine Verantwortungsdiffusion zu befürchten.

Statt beispielsweise eine neue Behörde für die administrative Kontrolle einzurichten, steht mit dem Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) bereits eine hinreichend unabhängige und mit umfassender Expertise ausgestattete Behörde zur Verfügung. Hierauf hat auch der Beauftragte selbst bereits hingewiesen.¹¹ Seine Befugnisse und vor allem seine Ausstattung sollten daher entsprechend ausgeweitet werden. Dabei muss freilich seine Unabhängigkeit gewahrt bleiben. Jedenfalls sollten die Kontrollmöglichkeiten besser verzahnt werden. Hierfür sollten Kooperationsmöglichkeiten nicht nur, wie in § 58 BNDG-E vorgesehen, allgemeine Fragen, sondern auch Einzelfälle betreffen können.

Auch das Nebeneinander von G10-Kommission und gerichtsähnlichem Kontrollorgan im UKr erzeugt Redundanzen. Beide Organe sollen eine gerichtsähnliche Rechtskontrolle ermöglichen und dadurch die stark eingeschränkten Rechtsschutzmöglichkeiten für die Betroffenen ausgleichen (vgl. Urteil, Rn. 273). Daher sollten die Kompetenzen und Aufgaben der G10-Kommission mit denen des UKr zusammengeführt werden. Dies würde die Effizienz der Kontrolle auch insofern erhöhen, als die G10-Kommission weit schwächer ausgestattet ist, als dies im Einklang mit den Anforderungen des BND-Urteils für den UKr vorgesehen ist.

Eine Zusammenführung der administrativen und der gerichtsähnlichen Kontrollorgane würde es überdies erleichtern, einen **Gesamtüberblick über die Überwachungstätigkeit** der Nachrichtendienste des Bundes zu erhalten. Die mit dem Investigatory Powers Act 2016 im Vereinigten

¹¹ Erste Positionierung des BfDI zum Gesetzentwurf der Bundesregierung, veröffentlicht auf https://netzpolitik.org/2020/bnd-gesetz-datenschutzbeauftragter-kritisiert-staatstrojaner-fuer-geheimdienste/#2020-10-12_BfDI_BND-Gesetz_Erste-Positionierung.

Königreich geschaffenen Strukturen zeigen, welches Potenzial hier besteht. In diesem Sinne sollte auch der bisher nicht geregelte Bereich HUMINT der Kontrolle durch den UKr unterstellt werden.

Jedenfalls sollte neben § 42 BNDG-E auch eine **Positivdefinition der Kompetenzen des administrativen Kontrollorgans** aufgenommen werden, da andernfalls Streitigkeiten mit dem BND über seine Kompetenzen absehbar sind.

Begrüßenswert wäre es auch, einer **Ombudsperson** die Vertretung der Rechte der Betroffenen zu übertragen, die aus Geheimhaltungsgründen nicht selbst an Verfahren zur Rechtskontrolle teilnehmen können, und das Verfahren kontradiktorisch auszugestalten.

4.3 Mangelnde Sanktionsmöglichkeiten

Eine wirksame Kontrolle bedarf auch entsprechender Sanktionsmöglichkeiten. Hier greift der Gesetzentwurf deutlich zu kurz. **Das Beanstandungsverfahren ist zu langwierig und schwerfällig, um effektiv zu sein.** Nicht nachvollziehbar ist, dass das Bundeskanzleramt gem. 52 BNDG-E gleich dreimal angehört werden muss, *vor* dem Ausspruch der Beanstandung gegenüber dem BND; innerhalb von drei Monaten *nach* der Beanstandung gegenüber dem BKAm, falls der BND nicht abgeholfen hat; und dann erneut *vor* der Entscheidung durch das gerichtsähnliche Kontrollorgan. Ein **Verwertungsverbot** für illegal erhobene Daten ist nicht vorgesehen. Auch für die Verletzung von Pflichten des BND zur Unterstützung des UKr aus § 56 BNDG-E ist keine Sanktionsmöglichkeiten vorgesehen.

4.4 Paralleler Ausbau der parlamentarischen Kontrolle nötig

Die parlamentarisch-politische Kontrolle des BND war nicht Gegenstand des Verfahrens vor dem Bundesverfassungsgerichts; die aus Art. 45d GG abgeleiteten parlamentarischen Befugnisse bleiben freilich von den grundrechtlich begründeten rechtlichen Kontrollbefugnissen unberührt (Rn. 300). Die parlamentarische Kontrolle durch das Parlamentarische Kontrollgremium (PKGr) ist gerade nicht auf die Rechtskontrolle begrenzt, sondern hat „eine eigene [...] Funktion und ist Ausdruck der allgemeinen parlamentarischen Verantwortung für die sachgerechte und politisch angemessene Aufgabenwahrnehmung der Exekutive“ (Urteil, Rn. 300).

In dem Maße wie die exekutiven Befugnisse und das Budget der zu kontrollierenden Behörde wachsen, müssen nicht nur die rechtlichen, sondern auch die faktischen Kontrollmöglichkeiten des Parlaments mitwachsen. Insofern gilt, was das Bundesverfassungsgericht für die angemessene personelle und sächliche Ausstattung und die nötigen Befugnisse der Rechtskontrolle ausführte (Urteil, Rn. 272 ff.), nicht minder für die parlamentarische Kontrolle. Diese dient keineswegs nur der Sicherung der Verantwortlichkeit der Exekutive gegenüber der direkt gewählten Volksvertretung. Sie ermöglicht dem Parlament auch, gesetzgeberisch nachzusteuern, wo Veränderungen in der Rechtswirklichkeit veränderte Rechtsgrundlagen für eine effektive rechtsstaatliche Überwachungstätigkeit erfordern. Eine enge Kopplung zwischen Behörde und Parlament kann insofern auch der Aufgabenerfüllung der Behörde selbst förderlich sein.

Bedauerlicherweise sieht § 55 BNDG-E eine verpflichtende Information des PKGr durch den UKr **nur alle sechs Monate** vor, und auch nur nach Anhörung des BKAm. Dies ist keine Verbesserung gegenüber der bisherigen Lage (§ 16 Abs. 6 BNDG). Hier erscheint eine deutlich häufigere Information notwendig.

Mit Blick auf die katastrophale Umgehung des parlamentarischen Kontrollrechts durch den BND, die die Snowden-Enthüllungen aufgedeckt haben, sollte die Informationspflicht in § 4 PKGrG mit einer **Sanktionsmöglichkeit** versehen werden. Die bloße Erwähnung im Bericht an den Bundestag gem. § 13 Satz 2 PKGrG hat sich als nicht effektiv erwiesen.

Zur Effektivierung der Kontrolle würde es auch beitragen, wenn die mit nachrichtendienstlichen Fragen befassten Gremien und Ausschüsse, wie PKGr, Vertrauensgremium, Innen-, Rechts-, Verteidigungs- und Auswärtiger Ausschuss, sowie die G 10-Kommission, das Art. 13 GG-Gremium, das ZfD-

Gremium und parlamentarische Untersuchungsausschüsse **gemeinsam zu relevanten Themen taugen** können.

Eine weitergehende parlamentarische Kontrolle ermöglichen Untersuchungsausschüsse gem. Art. 44 GG. In der Praxis kann allerdings eine exzessive **Einstufung als Verschlusssache** eine wirksame parlamentarische Kontrolle durch Untersuchungsausschüsse stark behindern. Daher sollte eine unabhängige, ständige Kontrollinstanz eingerichtet werden, die überprüft, ob Verschlusssachen ihre Einstufung verdienen.

5 Neue Eingriffsbefugnisse ohne Überwachungsgesamtrechnung

§ 19 Abs. 6 BNDG-E eröffnet dem BND die Möglichkeit, Zugang zu informationstechnischen Systemen eines ausländischen Telekommunikations- oder Telemediendiensteanbieters zu erlangen. Wenn ausländische Provider ihm also freiwillig keine Informationen übermitteln, sollen sie vom BND gehackt werden können. Auch hierbei handelt es sich um eine nachträgliche Legalisierung einer bereits seit Jahren existierenden Praxis.¹² Aufgrund der Weite der Ermächtigungsnorm könnten die darauf gestützten Hack-Angriffe bis hin zu einer Online-Durchsuchung reichen, die enorm hohe Grundrechtsrelevanz hat¹³. Das Bundesverfassungsgericht hat im BND-Urteil klargestellt: Die Grundrechte – auch das Computergrundrecht – gelten grundsätzlich auch bei hoheitlicher deutscher Aktivität auf ausländischem Territorium; lediglich ihre Reichweite kann variieren (Rn. 104). Insofern ist diese Ausweitung im Hinblick auf das in seiner Abwehrdimension (Rn. 105) betroffene sogenannte „Computergrundrecht“ aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG **verfassungsrechtlich höchst bedenklich**.

Besorgniserregend ist diese neuerliche Ausweitung der Befugnisse des BND auch mit Blick darauf, dass es bis heute an einer **Überwachungsgesamtrechnung fehlt**.¹⁴ Bevor immer neue Befugnisse für die Sicherheitsbehörden eingeführt werden, sollte zunächst ein Überblick der bestehenden gesetzlichen Regelungen erstellt und deren Wirksamkeit evaluiert werden. Dabei sollte auch eine Gesamtaufstellung der existierenden Kontrollmechanismen in ihrem Verhältnis zueinander erfolgen, um Lücken, Doppelungen und Ineffizienzen festzustellen. Ein Augenmerk sollte überdies auf informellen Kooperationen zwischen Polizeien und Geheimdiensten liegen, die bisher nicht normiert sind (z.B. GTAZ, GETZ), was auch bereits in der mündlichen Verhandlung vor dem Bundesverfassungsgericht zu kritischen Nachfragen des Gerichts geführt hat.

6 Fazit

Aus den vorgenannten Gründen hätte ein neues Bundesnachrichtendienstgesetz, wenn es in dieser Form verabschiedet würde, bei einer erneuten Überprüfung durch das Bundesverfassungsgericht wohl keinen Bestand. Folgende Punkte sollten daher im Gesetzgebungsprozess dringend nachgebessert werden:

1. Der Gesetzentwurf sollte um eine **Definition des Journalistenbegriffs** ergänzt werden, die auf Arbeitsweise, Freiheit und Unabhängigkeit abstellt. Die Gesetzesbegründung sollte auf entsprechende journalistische Standards verweisen. Der Gesetzentwurf sollte eine **Dokumentation der Entscheidung über die Schutzwürdigkeit von Vertraulichkeitsbeziehungen** vorsehen.

¹² Vgl. <https://www.spiegel.de/politik/deutschland/journalisten-spitzelaffaere-bnd-beobachtete-afghanischen-minister-farhang-a-549434.html>; <https://www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html>.

¹³ BVerfGE 120, 274 – *Online-Durchsuchung*.

¹⁴ Begriff bei Roßnagel, NJW 2010, 1238 (mit Bezug auf BVerfGE 125, 260 – *Vorratsdatenspeicherung*).

2. Der Gesetzgeber sollte die **Trennung zwischen personenbezogenen Inhalts- und Verkehrsdaten aufgeben** und einen umfassenden Schutz sicherstellen; als Vorbild kann das niederländische Recht dienen. Zumindest müssen § 26 und § 33 BNDG-E um einen **wirksamen Schutz von Vertraulichkeitsbeziehungen** i.S.d. § 21 Abs. 1 BNDG-E erweitert werden. Der Schutz von G10-Verkehren wird in § 26 Abs. 3 BNDG-E durch Ausnahmen vom Verarbeitungsverbot für verhashte Daten und „Maschine-zu-Maschine-Kommunikation“ ausgehöhlt; dies ist mit Art. 10 Abs.1 und Art. 5 Abs. 1 Satz 2 GG nicht vereinbar.
3. § 68 BNDG-E ist zur Erfüllung des **Zitiergebots** um Art. 5 Abs. 1 Satz 2 GG zu ergänzen.
4. Um eine **effektive Kontrolle von Selektoren** zu ermöglichen, sollten diese auch zu den gem. § 23 Abs. 2, 3 und 6 BNDG-E in der Anordnung aufzuführenden Informationen zählen. In § 23 und § 42 Abs. 1 BNDG-E ist eine gerichtsähnliche Vorabkontrolle für die Weitergabe von mit Selektoren erhobenen personenbezogenen Daten an ausländische Geheimdienste vorzusehen.
5. § 19 Abs. 10 BNDG-E sollte jedenfalls bei der Übermittlung an Inlandsgeheimdienste keinen **Ausschluss der Kennzeichnung der Daten** als aus der strategischen Fernmeldeaufklärung stammend vorsehen, da dies einer Umgehung der Übermittlungsvorgaben Tür und Tor öffnet.
6. Der Gesetzentwurf sollte vorschreiben, dass Absichtserklärungen des BND mit ausländischen Geheimdiensten gem. § 31 BNDG-E Vorkehrungen treffen, dass die „**third party rule**“ einer Kontrolle durch das UKr nicht entgegenstehen und eine Vorabkontrolle durch das UKr vorsehen.
7. Der Gesetzentwurf sollte in § 56 BNDG-E genaue Vorgaben zur **Ausgestaltung des Kontrollrechts** bei gemeinsamen Dateien und Räumen des BND und ausländischer Nachrichtendienste machen. Die Verweigerung des Zutritts oder Zugangs durch den BND gegenüber dem UKr sollte nicht an die Einschätzung des BND gekoppelt werden, dass dies für die Kontrolle erforderlich ist. Jedenfalls sollte diese Einschätzung selbst einer unabhängigen Kontrolle unterworfen werden.
8. **Gemeinsame Kontroll-Strukturen für die gesamte Fernmeldeaufklärung** könnten Synergien schaffen und effizienter arbeiten. Dies würde auch einen Gesamtüberblick über die Überwachungstätigkeit des Bundes erleichtern. Daher sollte über eine Einbindung oder weitergehende Kooperationsmöglichkeiten des BfDI ebenso nachgedacht werden wie eine Integration der G10-Kommission.
9. Parallel sollte die **parlamentarische Kontrolle ausgebaut** werden. Für das PKGr sind häufigere Berichte, Sanktionen und Kooperationsmöglichkeiten wünschenswert. Darüber hinausgehend sollte die Einstufung als Verschlussache einer Kontrolle unterworfen werden.
10. Neue geheimdienstliche Befugnisse sollten erst nach Durchführung einer **Überwachungsgesamtrechnung** eingeführt werden.