Stiftung
Neue
Verantwortung

Stellungnahme

im Rahmen der

Verbändebeteiligung zum Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts und des Bundesverwaltungsgerichts

Dr. Thorsten Wetzling und Kilian Vieth
Stiftung Neue Verantwortung e.V., Berlin

3. Dezember 2020

Gliederung

Einleitung

Wir bedanken uns für die Möglichkeit zur Stellungnahme. Mit dem Referentenentwurf werden zentrale Baustellen und Defizite der deutschen Nachrichtendienstkontrolle in Folge des Grundsatzurteils des Bundesverfassungsgerichts adressiert. Gerade bei einem sicherheitspolitisch und grundrechtlich so hochsensiblen Bereich wie der technischen Aufklärung gehört das Handlungsspektrum der Exekutive einer unabhängigen und wirkmächtigen Prüfung unterzogen. Die rechtsstaatliche Einhegung von Überwachungsbefugnissen und deren unabhängige Rechtskontrolle sind zentral für die demokratische Legitimation, die für die millionenfachen Eingriffe in die Grundrechte aus Art. 10 GG und Art. 5 GG vonnöten ist. Von daher ist es für uns wichtig, uns im Rahmen der kurzen Frist eingehend mit den vorgeschlagenen Veränderungen im Nachrichtendienstrecht zu befassen. Der Bundestag hat durch die vielen klaren verfassungsrechtlichen Vorgaben aus Karlsruhe eine einmalige Chance erhalten, bei dieser Novellierung international bedeutsame rechtsstaatliche Standards zu setzen. Bundesregierung und Bundestag haben, auch mit Blick auf die düstere Rolle deutscher Geheimdienste in der gesamtdeutschen Geschichte, eine besondere Verantwortung in Fragen der demokratischen Nachrichtendienstführung mit gutem Beispiel voran zu gehen.

Um es vorwegzunehmen: Der Referentenentwurf stellt im Vergleich zum aktuellen, verfassungswidrigen Status quo eine deutliche Verbesserung dar. Zukünftig würde es entscheidend verbesserte und ressourcenmäßig gestärkte Möglichkeiten geben, die Rechtmäßigkeit der strategischen Ausland-Fernmeldeaufklärung (§ 19 Abs. 1)[1] sowie die vielen Etappen der Datenverarbeitung und Übermittlungen unabhängig zu prüfen. Wir freuen uns, im Rahmen unserer fortlaufenden Arbeit an einem Kompendium zu guten Rechtsnormen und innovativer Kontrollpraxis im internationalen Vergleich,[2] neue vorbildliche Beispiele aus Deutschland aufnehmen zu können.

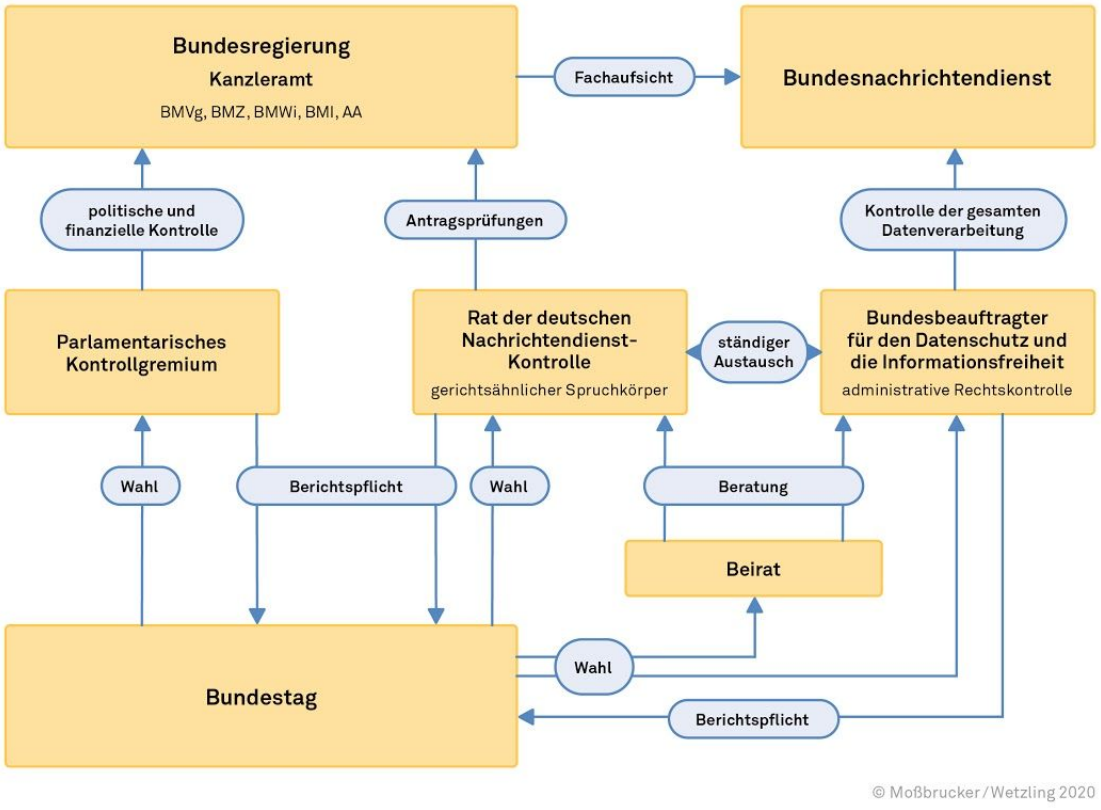
Dennoch greift der Entwurf an vielen Stellen zu kurz, beziehungsweise wird mit der unzureichenden Begrenzung einiger Überwachungsbefugnisse (zum Beispiel im Rahmen der Eignungsprüfung; siehe Abschnitt B) das Ziel einer rechtsstaatlichen Einhegung von Grundrechtseingriffen verfehlt.

Anders als in anderen Demokratien, ist ein einheitlicher und rechtsklarer Rahmen für das gesamte deutsche Nachrichtendienstrecht weiterhin nicht in Sicht. Es bleibt vielmehr auf zu vielen verschiedenen Gesetzestexten mit zahlreichen Querverweisen verteilt, was die Rechtsklarheit erheblich erschwert.[3] Dies zeigt sich jetzt auch daran, dass sowohl bei der Novellierung des BND-Gesetzes als auch bei der Novellierung des BVerfSch-Gesetzes zentrale Veränderungen am Artikel 10-Gesetz vorgenommen werden, die sich leichter erschließen ließen, wenn es einen einheitlichen Rechtsrahmen für das

[1] Hinweis: Wenn wir in diesem Dokument Paragraphen ohne weitere Nennung des Gesetzes zitieren, meinen wir damit die Paragraphen des Referentenentwurf vom 25.10.2020.
[2] Siehe Thorsten Wetzling und Kilian Vieth, "Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations", 2018, https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex5_CompendiumBulkSurveillance.pdf
[3] Hierzu zählt das BNDG, das BVerfSchG, das MADG, das Artikel 10-Gesetz, das Kontrollgremiumgesetz (PKGrG). Das Inhaltsverzeichnis der von der Bundestagsverwaltung herausgegebenen Gesetzessammlung Rechtsgrundlagen für die Tätigkeit und die Kontrolle der Nachrichtendienste des Bundes führt 31 verschiedene Gesetzestexte auf.

Nachrichtendienstrecht gäbe. Leider wird diese Chance nicht genutzt. Die Inland-Ausland Fernmeldeaufklärung nach § 5 Artikel 10-Gesetz bleibt weiterhin getrennt von der strategischen Ausland-Fernmeldeaufklärung normiert und kontrolliert. Dabei handelt es sich um eine ähnliche Praxis, mit ähnlichen Antrags- und Genehmigungsprozessen. Auch werden die gleichen Anbieter von den gleichen Stellen zur Ausleitung verpflichtet. Mit dem neuen unabhängigen Kontrollrat und der G10-Kommission bleiben aber zwei institutionell und befugnistechnisch gänzlich unterschiedlich aufgestellte Kontrollorgane mit ähnlich gelagerten Aufgaben betraut. Besser wäre es da gewesen, das ohnehin zu komplexe Nachrichtendienstrecht zu entrümpeln und der der Wirksamkeit der Kontrolle entgegenstehenden Fragmentierung der Aufsichtsgremien mit einer Reduktion der Gremien zu begegnen. Dafür hätte man einen einheitlichen Rechtsrahmen im BND-Gesetz für sämtliche Befugnisse der strategischen Fernmeldeaufklärung schaffen können und dabei die Rechtskontrolle allein dem unabhängigen Kontrollrat (ebenfalls im BND-Gesetz und nicht im Art. 10-Gesetz) übertragen können. Ähnlich wird dies auch in anderen Demokratien gehandhabt, wie z.B. den Niederlanden, Kanada und Großbritannien.

Den Leitlinien des Karlsruher Urteils folgend wäre es zum Beispiel möglich gewesen, die Nachrichtendienstkontrolle auf drei starke Institutionen zu beschränken (siehe Schaubild unten).[4] Dabei hätte man, auch um Doppelzuständigkeiten bei der Kontrolle weiter zu vermeiden, die gesamte administrative Rechtskontrolle und die Kontrolle der Einhaltung datenschutzrechtlicher Standards zukünftig dem oder der Bundesdatenschutzbeauftragten (BfDI) übertragen können.



[4] Siehe Thorsten Wetzling und Daniel Moßbrucker, "BND-Reform, die Zweite: Vorschläge zur Neustrukturierung der Nachrichtendienst-Kontrolle", 2020, https://www.stiftung-nv.de/sites/default/files/bnd_reform_die_zweite_vorschlaege_zur_neustrukturierung.pdf

Zudem lässt man die Chance verstreichen, dem Organ der unabhängigen Rechtskontrolle einen externen Beirat zur Seite zu stellen, wie es beispielsweise dem Technology Advisory Panel des Investigatory Powers Commissioners Office in Großbritannien gewährt wurde. Gerade mit Blick auf den umfassenden Wandel und die rapide Weiterentwicklung von Überwachungstechnologien wäre es unsere Meinung nach wichtig, in begrenzter Weise einen Austausch mit unabhängigen Expert:innen unterschiedlicher Fachrichtungen gerade für die Rechtskontrolle zu ermöglichen. Auch der notwendige strukturierte Informations- und Erfahrungsaustausch zwischen dem Unabhängigen Kontrollrat und dem oder der BfDI bleibt fortan zu unbestimmt.

Die nun vorgeschlagene Struktur der Nachrichtendienstkontrolle, die sich in diesem Referentenentwurf aber auch im bereits vom Kabinett beschlossenen Entwurf zur Harmonisierung des Verfassungsschutzrechts abzeichnet, führt daher unserer Meinung nach in der Gesamtheit dazu, dass die Durchschlagskraft der Kontrolle schwächer bleibt als sie es müsste.

A. Anmerkungen zu den Befugnissen und zur institutionellen Ausgestaltung der Rechtskontrolle (Unterabschnitt 5 des Referentenentwurfs; §§ 40 - 61)

1. Einleitung

Mit der vorliegenden Novellierung wird ein wichtiger Schritt in der deutschen Nachrichtendienstkontrolle unternommen. Erstmals wird neben der parlamentarischen Kontrolle und der unabhängigen Datenschutzkontrolle durch den oder die BfDI, die unabhängige Rechtskontrolle (§§ 40-61) in Gestalt des Unabhängigen Kontrollrats als oberste Bundesbehörde geschaffen. Trotz der im Folgenden erörterten Möglichkeiten, die Kontrollbefugnisse und die institutionelle Ausgestaltung der unabhängigen Rechtskontrolle deutlich effektiver zu gestalten, sind zahlreiche Veränderungen zum aktuellen Status zu begrüßen. Aufgrund der kurzen Frist zur Einreichung einer Stellungnahme werden wir uns allerdings vor allem auf Punkte konzentrieren, an denen der Referentenentwurf unserer Meinung nach noch verändert werden sollte. Für den Fall, dass dieser Entwurf vom Kabinett so am 16.12.2020 beschlossen wird, hoffen wir, dass im Rahmen der parlamentarischen Befassung noch die Möglichkeit besteht, einige Fragen weiter zu thematisieren.

Die Bündelung von gerichtsähnlicher und administrativer Rechtskontrolle in einem Kontrollorgan lässt sich grundsätzliche schon auch gut begründen. Im internationalen Vergleich zeigt sich, dass eine direkte institutionelle Verknüpfung zwischen Vorabprüfungen und Ex-post-Kontrollen die Wirksamkeit der Aufsicht erhöhen kann. Dem steht jedoch entgegen, dass das gerichtsähnliche Kontrollorgan seine Kontrollbefugnisse nur "im Rahmen der strategischen Ausland-Fernmeldeaufklärung" (§ 42 Abs. 1 und Abs. 2, jeweils Satz 1) einsetzen darf. Das administrative Kontrollorgan ist wiederum "für die Rechtskontrolle der Bereiche der technischen Aufklärung, die nicht der Rechtskontrolle durch das gerichtsähnliche Kontrollorgan unterliegen" zuständig. Das heißt der potenzielle Mehrwert der Bündelung in einer Institution wird durch die getrennten Kontrollzuständigkeiten konterkariert.

1.1 Fehlende Kontrollbefugnisse im Rahmen der Rechtmäßigkeitsprüfung

Die "Katalogzuständigkeiten" der beiden Abteilungen des Unabhängigen Kontrollrats haben diverse Lücken, die die folgende Tabelle ohne Anspruch auf Vollständigkeit zusammenfasst.

Prüfgegenstand	Zuständigkeit des administrativen Kontrollorgans	Zuständigkeit des gerichtsähnlichen Kontrollorgans
Einblick in alle Suchbegriffe	Nein	Nein
Zugang zu gemeinsam geführten Dateien und IT- Systemen	Nein	Nein
Verarbeitung von Verkehrsdaten	Zu unbestimmt	Teilweise
Eignungsprüfung	Nein	Nein
Erhebung von Sachdaten ohne Personenbezug	Nein	Nein
Dateianordnung für gemeinsame projektbezogene Dateien die der BND nicht führt	Nein	Nein

2. Anmerkungen zum administrativen Kontrollorgan

Neben den Entscheidungen, die das gerichtsähnliche Kontrollorgan im Rahmen des Genehmigungsverfahrens zu treffen hat, hängt die Rechtmäßigkeit der technischen Aufklärung auch entscheidend davon ab, wie die rechtlichen Vorgaben und Schutznormen in der Praxis der Datenverarbeitung umgesetzt werden. Unser Meinung nach greift der Entwurf gerade bei den Katalogzuständigkeiten des administrativen Kontrollorgans zu kurz. Der Umfang, die Kontrollziele und die Technologie, die im Rahmen der administrativen Rechtskontrolle zum Einsatz kommen soll, bleiben zu unbestimmt. Bei zu vielen offenen Fragen erscheinen zukünftige Streitigkeiten vorprogrammiert, wenn zukünftig Beamt:innen in Vollzeit – und nicht wie aktuell ehrenamtliche Mitglieder wie bei der G10-Kommission oder teilzeitbeschäftige Mitglieder des Unabhängigen Gremiums – der anspruchsvollen und umfassenden Tätigkeit der administrativen Rechtskontrolle nachgehen sollen.

Da die administrative Rechtskontrolle dem Entwurf zufolge nicht, wie von einigen vorgeschlagen, den erfahrenen Referaten des oder der BfDI zugeschlagen wird, entsteht eine Parallelstruktur bzw. wird eine Doppelkontrolle in Kauf genommen. Dem oder der BfDI wird zukünftig keine der bestehenden Prüfkompetenz abgenommen aber es kommen auch keine Kompetenzen dazu. Vor diesem Hintergrund ist auch der Austausch und die Zusammenarbeit zwischen BfDI und dem administrativen Kontrollorgan unzureichend spezifiziert bzw. abgegrenzt worden.

2. 1. Fehlende und unkonkrete “Katalogzuständigkeiten”

Bei der Auflistung der Zuständigkeiten des administrativen Kontrollorgans sollte unbedingt ergänzt werden, dass die Kontrollbefugnis sich zumindest stichprobenartig auf die zahlreichen Maßnahmen erstreckt, die im Rahmen der Eignungsprüfung (§ 24 – siehe dazu auch den Abschnitt B) durchgeführt werden.

Zu § 51 Abs. 1 steht in der Begründung (S. 123): “Der administrative Kontrollkörper ist so auszugestalten, dass dieser eigeninitiativ stichprobenmäßig den gesamten Prozess der technischen Aufklärung von Ausländern im Ausland auf seine Rechtmäßigkeit prüft”. Das ist zu begrüßen und sicher auch ein bedeutsamer Fortschritt zum Unabhängigen Gremium, das häufig vor verschlossenen Türen stand. Dennoch werden aber auch hier, trotz der zahlreichen Vorgaben bezüglich der Sicherheitsüberprüfungen und der stark begrenzten Informationsflüsse in den parlamentarischen Raum, unnötige Grenzen der Kontrollbefugnisse gezogen. Das ist unverständlich, gerade wenn anderswo im Begründungstext hervorgehoben wird, dass den Kontrollierten “ein einheitliches Organ gegenüber[steht], welches in den hoch sensiblen Bereich der Informationen ausländischer Nachrichtendienste Einsicht nehmen kann” (S. 113).

Anders als bei einer auf funktionale Ziele ausgerichteten Rechtskontrolle sieht der Entwurf für das administrative Kontrollorgan lediglich eine Beobachterrolle vor, die auch häufig gegenüber dem gerichtsähnlichen Kontrollorgan zurücktritt. Es “unterstützt” letzteres und hat nur für “Bereiche der technischen Aufklärung, die nicht der Rechtskontrolle durch das gerichtsähnliche Kontrollorgan unterliegen” (§ 51 Abs. 1) eine eigene Befugnis. Es kann auch nur die “Rechtmäßigkeit von Suchbegriffen überprüfen, soweit nicht die originäre Zuständigkeit des gerichtsähnlichen Kontrollorgans eröffnet ist". Warum diese Entweder-Oder-Logik gewählt wurde, obwohl die administrative und die gerichtsähnliche Rechtskontrolle zwei Arme derselben Behörde werden sollen, erschließt sich uns nicht.

Um eine wirksame Ende-zu-Ende Kontrolle des Gesamtprozesses der Auslands-Fernmeldeaufklärung zu gewährleisten, sollte die administrative Kontrolle ausdrücklich für alle Datenverarbeitungsschritte eine Prüfkompetenz erhalten, auch wenn die gerichtsähnliche Kontrolle bereits involviert ist bzw. war. Die Kontrollbefugnis ist also nicht in Abgrenzung zu anderen Kontrollgremien zu definieren, sondern funktional, entlang des zu erreichenden Kontrollziels.

Zudem müsste dringend geklärt werden, ob für Fälle, in denen das gerichtsähnliche Kontrollorgan eine “originäre Zuständigkeit” hat aber keine Suchbegriffe zu sehen bekommt (siehe 3.1), dem administrativen Kontrollorgan ebenfalls – wegen der fehlenden originären Zuständigkeit – der Zugang zu den Suchbegriffen verwehrt bliebe (§ 51 Abs. 1 Satz 2).

Die einem funktionalen Kontrollmandat (Ende-zu-Ende Kontrolle) eher entgegenlaufende Abgrenzung der originären Zuständigkeiten kommt auch zum Ausdruck in § 51 Abs. 2 wonach das gerichtsähnliche Kontrollorgan den Prüfauftrag des administrativen Kontrollorgans bestimmt. Hier wäre es unserer Meinung nach zielführender, wenn das administrative Kontrollorgan selbständig den Prüfauftrag und seine Kontrollziele und Prioritäten bestimmen könnte. Diese explizite Unterordnung der administrativen Rechtskontrolle unter den Spruchkörper läuft unserer Meinung auch der Intention des

Karlsruher Grundsatzurteils zuwider, worin explizit eine "eigeninitiative" und "unabhängige" Prüfkompetenz für den "gesamten Prozess der strategischen Überwachung" gefordert wurde (Rn. 276). Eine weitere Degradierung des administrativen Kontrollorgans sehen wir in dem Beanstandungs-Prozess-Marathon, der in 2.3 erläutert wird.

Dem Begründungstext zu § 51 Abs. 1 ist zu entnehmen, dass es dem gerichtsähnlichen Kontrollorgan unbenommen bleibt, "auf die Expertise des administrativen Kontrollorgans zuzugreifen". Hier wäre es besser, die Holschuld in eine Bringschuld umzuwandeln. Damit könnte dem Ziel in der Gesetzesbegründung unserer Meinung besser entsprochen werden, "zwischen beiden Säulen ein[en] offene[n] und unmittelbare[n] Austausch" zu gewährleisten (Seite 114).

Anstatt die Prüftätigkeiten im Vorfeld einer strengen Hierarchie zu unterwerfen, hätte man mehr Mühe aufbringen können, um die konkreten Prüftätigkeiten und Ziele der administrativen Kontrolle zu benennen.

2. 2. Zugang

Umfassender Datenzugang ist elementar für eine wirksame Kontrolle. Daher ist es zu begrüßen, dass dem Unabhängigen Kontrollrat nach § 56 Abs. 3 jederzeit Zutritt zu sämtlichen Dienststellen und Zugang zu sämtlichen informationstechnischen Systemen gewährt werden soll.

Diese grundsätzliche Verbesserung zum Status quo wird allerdings dadurch eingeschränkt, dass der Zugriff auf Suchbegriffe (siehe Abschnitt 3.1 unten) und auf Daten aus der Eignungsprüfung und auf (unselektierte) Daten im Rahmen von internationalen Kooperationen weiter lückenhaft bleibt. In der Begründung wird dazu ausgeführt: "Vom Bundesnachrichtendienst verarbeitete Daten, die ausschließlich in IT-Systemen gespeichert sind, welche ihrerseits nicht der alleinigen Verfügungsbefugnis des Bundesnachrichtendienstes unterliegen, sind dennoch [...] vollumfänglich kontrollierbar: Diese werden für Kontrollzwecke durch den Bundesnachrichtendienst in eigene IT-Systeme des Bundesnachrichtendienstes kopiert und können dort eingesehen und geprüft werden" (S. 126). Diese Klarstellung sollte im Sinne der Nachvollziehbarkeit, dass die Third-Party-Rule die Kontrolle nicht behindern darf, als separate Kontrollbefugnis in den Gesetzestext aufgenommen werden.

Wie in vielen Ländern bereits praktiziert, braucht eine effektive Datenschutzkontrolle insbesondere den umfassenden, direkten Zugang zu den Protokolldaten, die entlang der verschiedenen Stufen des Verarbeitungsprozesses anfallen (z.B. Log-Files für Filterfehler, Zweckänderungen, Übermittlungen und Löschung). Diese Daten müssen der Rechtskontrolle in einer aussagekräftigen und maschinenlesbaren Form zur Verfügung stehen, um effiziente datenbasierte Kontrolle überhaupt erst zu ermöglichen. Das wäre durch die Schaffung einer Audit-Trails-Pflicht sicherzustellen: Protokolldaten müssen beim BND so geführt und gepflegt werden, dass sie den Bedürfnissen der administrativen Rechtskontrolle entsprechen.

Eine gesetzliche Verpflichtung zur Aufzeichnung und Bereitstellung aussagekräftiger Protokolldateien sowie eine umfassende Datenkennzeichnungspflicht könnten ohne großen

Aufwand in den Gesetzentwurf integriert werden. Insbesondere bei den vielen vorgesehenen Abwägungsentscheidungen z.B. bei der gezielten Erhebung von personenbezogenen Daten (§ 19 Absatz 5 i.V.m. § 20), beim Schutz von Vertraulichkeitsbeziehungen (§ 21) und beim Kernbereichsschutz (§ 22) dürfen die Protokolldaten bisher jeweils "ausschließlich zur Durchführung von Kontrollen der Datenverarbeitung, einschließlich der Datenschutzkontrolle verwendet werden". Das betrifft ja allein die dienstinternen Prüfungen. Dabei würde nicht nur der BND, sondern auch die Organe der Rechtskontrolle enorm von der strukturierten Bereitstellung von Protokolldaten profitieren.[5] Die Protokollierungspflichten sollten daher im Gesetz detaillierter und umfassender gefasst werden. Da Log-Files bereits für andere Zwecke im Nachrichtendienstwesen aufgezeichnet und genutzt werden, sind die Bedürfnisse der Kontrolleur:innen bei der Konzeption der Logging-Systeme gezielt zu berücksichtigen.

Hier wäre daher eine Ergänzung im Entwurfstext denkbar, wonach die Protokolldaten auch der Rechtskontrolle uneingeschränkt zur Prüfung bereitzustellen sind. Gemeinsam mit dem BND sollten zudem die Mindestanforderungen an die Protokolldaten auch unter Beteiligung der Rechtskontrolle konzipiert werden. Das würde die Wirkmächtigkeit der Rechtskontrolle stärken.

2. 3. Umständliches Beanstandungsverfahren

Gegenwärtig sind im Entwurf deutlich zu viele Hürden auf dem Weg zur Beanstandung enthalten. Der vorgesehene Prozess sieht folgende langwierige Schritte vor:

(1) Beanstandungen bedürfen einer Vorab-Anhörung des BND (§ 52 Abs. 1)
(2) Bei Nicht-Abhilfe ist dann ein Vortrag beim Bundeskanzleramt vonnöten (§ 52 Abs. 2)
(3) Das Bundeskanzleramt kann zur Beanstandung eine Stellungnahme verfassen, auf die das gerichtsähnliche Kontrollorgan wiederum bis zu drei Monate warten müsste (§ 52 Abs. 3)
(4) Die Beanstandung kann erst dann dem gerichtsähnlichen Kontrollorgan vorgelegt werden (§ 52 Abs. 3)
(5) Vor einer Entscheidung durch das gerichtsähnliche Kontrollorgan muss dann erneut das Bundeskanzleramt angehört werden (§ 52 Abs. 4 i.V.m. § 42 Abs. 4 Nr. 3)
(6) Der Kontrollrat kann erst dann "unter Beachtung des Geheimschutzes in abstrakter Weise" und nach erneuter (!) Anhörung des Bundeskanzleramtes den Deutschen Bundestag über Beanstandungen unterrichten. Zusätzlich kann das Bundeskanzleramt eine Stellungnahme beifügen (§ 55 Abs. 3).

Dieses langwierige Verfahren sollte im Sinne der Kontrolleffizienz deutlich abgekürzt werden. Außerdem bleibt offen, welche Sanktionsmöglichkeiten der Unabhängige Kontrollrat hat, wenn auch nach der Entscheidung, dass ein rechtswidriger Zustand vorliegt, keine Abhilfe geschaffen wurde. In Frage käme dafür z.B. die Beanstandung und deren Lösungsansätze nicht nur in die Unterrichtung des Bundestags zu integrieren, sondern auch – unter Wahrung der Geheimhaltung – in einer eigenständigen öffentlichen Berichtspflicht aufzunehmen.

[5] Vieth und Wetzling, "Datenbasierte Nachrichtendienstkontrolle: Agenda für mehr Wirksamkeit", S. 23ff, 2020, https://www.stiftung-nv.de/sites/default/files/datenbasierte_nachrichtendienstkontrolle.pdf

→ **Bessere Praxis:** Das norwegische Kontrollgremium EOS berichtet regelmäßig öffentlich über rechtswidrige bzw. beanstandete Fälle, z.B. bei der technischen Datenerfassung des Dienstes.[6]

3. Weitere Punkte zur unabhängigen Rechtskontrolle

3. 1. Einblick in alle Suchbegriffe gesetzlich verankern

Vor dem Hintergrund, dass der BND im Ausland Kommunikation zu einem erheblichen Anteil heimlich in ausländischer Telekommunikationsinfrastruktur oder bei ausländischen Diensteanbietern erhebt, ist die unabhängige Prüfung und Genehmigung aller verwendeten Suchbegriffe durch den Unabhängigen Kontrollrat dringend geboten.

Allerdings wurde dem Unabhängigen Kontrollrat im vorliegenden Gesetzentwurf der Zugriff auf Suchbegriffe fast gänzlich entzogen. § 20 "Besondere Formen der strategischen Ausland-Fernmeldeaufklärung" hieß im letzten öffentlich bekannten Referentenentwurf noch "Besondere Formen der Verwendung von Suchbegriffen"[7]. Genauso sind bei der Norm zu Anordnungen (§ 23 Abs. 5 bis Abs. 7) nun alle Hinweise auf Suchbegriffe entfernt worden. Lediglich das administrative Kontrollorgan dürfte "soweit nicht die originäre Zuständigkeit des gerichtsähnlichen Kontrollorgans eröffnet ist, die Rechtmäßigkeit von Suchbegriffen überprüfen" (§ 51 Abs. 1).

Daher ist zu betonen: für eine effektive Prüfung der Anordnungen von strategischen Aufklärungsmaßnahmen, braucht der unabhängige Kontrollrat Zugang zu allen dabei verwendeten Suchbegriffen. Wenn der im Entwurf geplante Unabhängige Kontrollrat diese Suchbegriffe nicht einsehen kann, kann er sie auch nicht kontrollieren. Die Prüfung der rechtmäßigen Erfassung von Inhalten allein anhand von abstrakten "strategischen Aufklärungsmaßnahmen" (§ 23 Abs. 1 i.V.m. § 42 Abs. 1 Nr. 1) oder "Zielen" (§ 23 Abs. 5 i.V.m. § 42 Abs. 1 Nr. 2) bleibt dann zwangsläufig oberflächlich und lückenhaft.

Deswegen sollte der Zugriff auf Suchbegriffe dringend ausgeweitet statt gestrichen werden. In § 10 Artikel 10-Gesetz wird die Nennung von Suchbegriffen in Anordnungen bereits verlangt (darüber hinaus das Gebiet, über das Informationen gesammelt werden sollen, und die Übertragungswege, die der Beschränkung unterliegen). Da der Geltungsbereich des Art. 10 GG auch für die strategische Fernmeldeaufklärung eröffnet ist, bleibt unklar, warum die Regelung in § 23 des Entwurfs hinter diesen Vorgaben des § 10 Artikel 10 Gesetzes zurückbleiben sollte.

3. 2. Unabhängigkeit des Kontrollrats

Die Mitglieder des Kontrollrats sollen laut Entwurf auf Vorschlag der Präsident:in des BGH und der Generalbundesanwält:in vom Parlamentarischen Kontrollgremium des Bundestages gewählt werden (§ 43 Abs. 1 und 3). Hierbei sollte dem PKGr jedoch eine tatsächliche Auswahl an Kandidat:innen für die Besetzung des Kontrollrats zur Verfügung stehen. Es

[6] EOS-Gremium, "Annual Report (2017-2018)", S. 24f, 2018, https://eos-utvalget.no/wp-content/uploads/2019/05/eos_annual_report_2018.pdf
[7] Meister und Biselli, "Eine neue Lizenz zum Hacken", 29.09.2020, https://netzpolitik.org/2020/bnd-gesetz-eine-neue-lizenz-zum-hacken/

sollte also ein Pool an vorgeschlagenen Mitgliedern geben, anstatt nur eine vorgeschlagene Liste an Mitgliedern bestätigen zu können.

Obwohl das BND Urteil die Bedeutung der richterlichen Unabhängigkeit für die Kontrollstruktur an vielen Stellen betont hat (Rn. 275, 281, 282, 286), soll es dem Entwurf nach bei einer Einbeziehung von Bundesanwält:innen bleiben (§ 43 Abs. 1).

Die Integration der Strafverfolger:innen in das quasi-gerichtliche Organ – auch wenn die Pfadabhängigkeit vom Unabhängigen Gremium zum Unabhängigen Kontrollrat augenscheinlich ist – steht der geforderten richterlichen Unabhängigkeit entgegen. Um diese zu gewährleisten, wäre es überzeugender, den Kontrollrat ausschließlich mit (Bundes-)Richter:innen zu besetzen.[8] Dann würden sich auch die etwas umständlichen Verfahrensregelungen erübrigen, nach denen die Richter:innen im Spruchkörper mehrheitlich vertreten sein müssen (§ 49 Abs. 3) und die richterlichen Mitglieder bei Stimmengleichheit entscheiden (§ 49 Abs. 4 Satz 5).

→ **Bessere Praxis:** Wenn bei der Prüfung einer Anordnung nur eine Sichtweise auf die jeweiligen Rechtsfragen vertreten ist, besteht die Gefahr strukturell einseitiger Entscheidungen. Daher kann der US-amerikanische Foreign Intelligence Surveillance Court (FISC) eine Person ernennen, die als Amicus Curiae ("Freund des Gerichts") die Prüfung von Anordnungen unterstützt, die nach Ansicht des Gerichts eine neuartige oder bedeutsame Rechtsauslegung darstellen. Das US-Gesetz fordert ausdrücklich, dass die ernannten Gutachter:innen "rechtliche Argumente vorbringt, die den Schutz der persönlichen Privatsphäre und der bürgerlichen Freiheiten fördern." (50 U.S. Code § 1803(i)(4)(A), eigene Übersetzung). Ähnlich verfährt Schweden: Bei allen Verfahren vor dem schwedischen Gericht für Auslandsaufklärung (UNDOM) muss eine Datenschutzbeauftragte anwesend sein, es sei denn die Operation würde dadurch verzögert oder gefährdet.[9]

3. 3. Internationale Kooperation von Kontrollgremien

Den meisten Aufsichtsbehörden fehlen Mechanismen, um zu prüfen, ob und wie die nationalen Nachrichtendienste Daten an ausländische Stellen weitergeben, und ob Anforderungen wie Zweckbindungen dabei eingehalten werden. Deswegen brauchen Kontrollbehörden, wie der im Entwurf vorgesehene Unabhängige Kontrollrat, ein klares Mandat für die internationale Kooperation mit anderen Kontrollgremien.[10]

Dieses Problem der fehlenden Kontrollbefugnis für in Dateien gespeicherte Daten und IT-Systeme, die nicht *alleine* dem BND unterliegen, bleibt im Entwurf bestehen. Eine Rechtsgrundlage für den strukturierten Austausch zwischen Kontrollbehörden sollte genau dort ansetzen. Zum Beispiel wenn eine Datenbank nicht in "alleiniger Verfügungsberechtigung des Bundesnachrichtendienstes [steht]" (§ 56 Abs. 3), kann die

[8] Um eine enge Rückbindung an die richterliche Praxis zu gewährleisten, kämen dafür auch Richter von (Ober-)Landgerichten in Frage. Vgl. Sensburg, "Is SIGINT coming to an end?", 30.11.2020, About:Intel, https://aboutintel.eu/high-hurdles-for-bnd/

[9] Lubin, "Legitimizing Foreign Mass Surveillance in the European Court of Human Rights", Just Security, 2. August 2018, https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/

[10] de Ridder, "A simple yet existential demand: let oversight bodies work together", 6.11.2019, https://aboutintel.eu/simple-oversight-demands/ und weiterführend: https://aboutintel.eu/oversight-cooperation/

Kooperation der zuständigen Aufsichtsgremien dabei helfen, eine kontinuierliche Kontrolle zu sichern.

Ansätze für die strukturierte Zusammenarbeit von Kontrollbehörden bestehen mehrere: insbesondere hat sich die Zusammenarbeit zwischen einigen europäischen Aufsichtsbehörden weiterentwickelt. Offiziell beteiligen sich sechs Kontrollgremien aus Belgien, Dänemark, den Niederlanden, Norwegen, der Schweiz und Großbritannien daran. Die Gruppe arbeitet daran, gemeinsam abgestimmte Kontrollen durchzuführen, um ein besseres Bild der internationalen Nachrichtendienstkooperation und des oft automatisierten Datenaustausches zu erhalten, die ansonsten für eine Aufsichtsbehörde viel schwieriger oder gar nicht zu untersuchen wären.

Damit diese essentielle Beteiligung des Unabhängigen Kontrollrats an internationaler Kontrollkooperationen nicht an formalen Hürden scheitert, ist eine Rechtsgrundlage für die Teilnahme an internationaler Zusammenarbeit in den Entwurf aufzunehmen. Gerade die administrativen, also "nicht-politischen" Kontrollorgane profitieren von dieser Kollaboration. Ein ähnlich gelagerter Zusammenschluss besteht auch zwischen den administrativen Kontrollbehörden der FiveEyes-Mitglieder im sogenannten "Five Eyes Intelligence Oversight and Review Council (FIORC)"[11].

3. 4. Inländische Zusammenarbeit von Kontrollgremien

Kooperation zwischen inländischen Kontrollbehörden ist im vorliegenden Entwurf verankert (§ 58), jedoch viel zu unspezifisch. Angesichts der vielen, sich mitunter überschneidenden, Kontrollzuständigkeiten des Unabhängigem Kontrollrats, des Parlamentarischem Kontrollgremiums, der G10-Kommission und dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, sowie des oder der Ständigen Bevollmächtigten in der Bundestagsverwaltung, und ungeachtet der Art. 13 Kommission, muss die Zusammenarbeit konkreter bestimmt werden, um praktikabel zu sein.

Alleine mit dem Hinweis, die sehr unterschiedlich aufgestellten Gremien können sich "im Rahmen ihrer jeweiligen Kontrollzuständigkeit über allgemeine Angelegenheiten ihrer Kontrolltätigkeit austauschen" (§ 58 Abs. 1), ist es sicher nicht getan. Worüber genau sollen sich die Aufsichtsgremien wie häufig in welcher Form austauschen? In der Praxis haben sich schon konkreter Modelle eingestellt, zum Beispiel die gemeinsamen Kontrollbesuche beim BND durch die G10-Kommission und BfDI.

Was sind die Ziele und Aufgaben bei der Zusammenarbeit gerade mit Blick auf die sich überschneidenden Zuständigkeiten von

- BfDI und administrativer Rechtskontrolle,
- BfDI und gerichtsähnlichem Kontrollorgan,
- administrativer Rechtskontrolle und G10-Kommission, und
- gerichtsähnlichem Kontrollorgan und G10-Kommission?

[11] Siehe z.B. Office of the Inspector General of the Intelligence Community, "Semiannual Report", S. 10, https://www.dni.gov/files/documents/FOIA/OCT2017-MAR-2018_SAR_FINAL.PDF; ebenso: Charter of the Five Eyes Intelligence Oversight and Review Council, https://www.igis.gov.au/sites/default/files/2020-05/fiorc_charter_-_signatures_removed.pdf

In Frage kommen zum Beispiel gemeinsame Schulungen, gemeinsam abgestimmte Prüfaufträge, gemeinsam genutzte Ressourcen (technisch geschultes Personal, Expertenbeiräte), abgestimmte Prioritätensetzung bei der Jahresplanung der Kontrolltätigkeiten, gemeinsame Evaluationen, gemeinsame Berichterstattungen und Austausch von Personal zur Weitergabe von Prüferfahrungen und Fachwissen.

In diesem Zusammenhang ist auch die Regelung von Sanktionsmöglichkeiten zu betrachten. Das Befragungsrecht in § 56 Abs. 4 wird im Begründungstext dahingehend eingeordnet, dass der Unabhängige Kontrollrat "beschäftigte Angehörige des Bundesnachrichtendienstes befragen oder von ihnen schriftliche Auskünfte einholen [kann]. Es besteht die Pflicht zur vollständigen und wahrheitsgemäßen Auskunft. Diese Pflicht ist von einer Zeugenvernehmung im Sinne eines Strafverfahrens oder im Kontext eines Untersuchungsausschusses zu unterscheiden, an die spezifische Sanktionen geknüpft sind, §§ 48 ff. StPO, 20ff. PUAG" (S. 126). Auch hier wäre zumindest an eine ähnlichlautende Sanktionierungsmöglichkeit zu denken.

3. 5. Kontinuierliche Rechtskontrolle

Eine kontinuierliche Rechtskontrolle, wie sie vom Bundesverfassungsgericht gefordert wurde (Rn. 272), muss die Prüfung der gesamten Datenverarbeitung und der vielen schwierigen Abwägungsentscheidungen beim Schutz von Journalist:innen, Berufsgeheimnisträger:innen oder beim Kernbereichsschutz ganzheitlich und strukturiert in den Blick nehmen. Viele der angedachten Schutzvorschriften, für die immer auch Ausnahmen vorgesehen sind, laufen sonst Gefahr, in der Praxis nicht zu greifen. Vor diesem Hintergrund irritiert es, dass gerade das Wort kontinuierlich aus § 40 gestrichen wurde. Der erste Entwurf betonte explizit, dass eine Kontrolle des Gesamtprozesses der technischen Aufklärung sichergestellt werden muss. In Kanada (NSIRA) und Großbritannien (IPCO) haben die Kontrollbehörden ganzheitliche und behördenübergreifende Mandate, die nicht auf einen Katalog einzelner Aufklärungsmaßnahmen beschränkt sind.

§ 42 Abs. 1 erlaubt dem Unabhängigen Kontrollrat lediglich die Kontrolle der technischen Aufklärung von Ausländern im Ausland durch den Bundesnachrichtendienst. Die Liste an Prüfzuständigkeiten umfasst dabei weder die Erhebung von Verkehrsdaten, noch die Eignungsprüfung (§ 24), noch die sonstige Erhebung von Sachdaten ohne Personenbezug. Allein im BND Gesetz sollen vier verschiedenen Anordnungstypen (§ 23 Abs. 1, § 23 Abs. 5, § 25 Abs. 1, § 37 Abs. 1) geschaffen werden. Dazu kommen die Anordnungen gemäß §§ 3, 5 oder § 8 des Artikel 10 Gesetzes. Das macht deutlich, dass die stringente Kennzeichnung der Inhalts- und Verkehrsdaten zum Zwecke der Kontrolle unausweichlich ist. Die Kontrollbefugnisse dürfen dazu nicht unnötig eingeengt werden und der Unabhängige Kontrollrat muss auf alle Daten, die der BND verarbeitet Zugriff haben und es muss ihm möglich sein, überhaupt einen Überblick über alle laufenden und geplanten Datenerfassungen zu gewinnen.

→ **Bessere Praxis:** Das dänische Kontrollgremium TET erstellt jährlich eine Übersicht aller nachrichtendienstlichen Datenverarbeitungssysteme der dänischen Dienste. Wenn es auf einzelne Erhebungsmethoden oder Anordnungstypen beschränkt wäre, wäre eine unabhängige Kartierung und Priorisierung aller Speicherorte, Server, IT-Systeme und Software mit denen die Dienste Daten sammeln, aufbewahren oder analysieren unmöglich.

Die Unabhängigkeit der Kontrolle wird geschwächt, da sie von der Bereitstellung von Informationen durch die Dienste abhängig bleibt.[12]

3. 6. Berichtspflichten

Eine öffentliche, informierte Diskussion ist eine demokratische Notwendigkeit für Vertrauen in die Arbeit staatlicher Stellen, insbesondere für solche, die tief in Grundrechte eingreifen. Daher ist es im Rahmen des Geheimschutzes für alle Aufsichtsgremien wichtig, regelmäßige Tätigkeitsberichte zu verfassen, die dem Bundestag und der interessierten Öffentlichkeit einen Überblick über das gesamte Spektrum der verschiedenen Kontrolltätigkeiten geben. So lässt sich dann auch über einen längeren Zeitraum hinweg erkennen, wie sich die Kontrolle verändert, welche Erfolge erzielt wurden und welchen Einfluss die Aufsichtstätigkeiten auf das Regierungshandeln gehabt haben.

Anders als bei der G10-Kommission, die gegenwärtig keine Berichtspflicht hat und wo stattdessen gemäß § 14 Abs. 1 Satz 1 Art. 10 Gesetz das für die "Beschränkungsmaßnahmen" zuständige Bundesministerium dem PKGr über diese Überwachungsmaßnahmen unterrichtet, ist es zu begrüßen, dass der Unabhängige Kontrollrat in Abständen von maximal sechs Monaten dem PKGr über seine Tätigkeit berichten soll (§ 55 Abs. 1). Es ist wichtig, dass die Kontrollorgane selbständig einen umfassenden Tätigkeitsbericht verfassen können – und bei Ihren Entscheidungen nicht, wie bei der G10-Kommission, auf von den Ministerien vorformulierte Textbausteine zurückgreifen müssen.

§ 55 Abs. 1 versäumt es aber, anders als zum Beispiel § 13 Satz 2 PKGR-Gesetz, die Inhalte der Tätigkeitsberichte näher zu bestimmen. Trotz des notwendigen Geheimschutzes sollte der Bericht des Unabhängigen Kontrollrats an das PKGr einen präzisen Überblick über das Antragsverfahren und seine Entscheidungen geben. Das betrifft einerseits die Anzahl der Anträge pro Kalenderjahr inklusive der zugrunde liegenden Rechtsgrundlage, die Anzahl der Genehmigungen (mit und ohne Vorbehalt) sowie die Zahl der abgelehnten Anträge samt Überblick der Ablehnungsgründe.

→ **Bessere Praxis:** Warum das wichtig ist, zeigt der Blick auf die Praxis in den Niederlanden. Dort hat das für die Genehmigungen von Überwachungsmaßnahmen zuständige Gremium TIB in seinem übrigens stets auch auf Englisch veröffentlichten Bericht kürzlich die Öffentlichkeit darüber informiert, dass es "in der Zeit vom 1. Mai 2018 bis zum 1. April 2019 insgesamt 2.159 Anträge" geprüft habe.[13] Zudem hat TIB in seinem Bericht die Anzahl der abgelehnten Anträge samt Ablehnungsgrund aufgeführt – dies allerdings zusammengenommen für beide Nachrichtendienste AIVD und MIVD. Dem Bericht lässt sich beispielsweise entnehmen, wie oft Anträge aus welchem Grund für unzulässig befunden und abgelehnt wurden.[14] Zudem erörtert der Bericht des TIB Beispiele für

[12] Vieth und Wetzling, "Datenbasierte Nachrichtendienstkontrolle: Agenda für mehr Wirksamkeit", 2020, S. 38f, https://www.stiftung-nv.de/sites/default/files/datenbasierte_nachrichtendienstkontrolle.pdf

[13] Jahresbericht der niederländischen Aufsichtsbehörde TIB, abrufbar unter: https://www.tib-ivd.nl/binaries/tib/documenten/jaarverslagen/2019/04/25/annual-report-2018-2019/TIB+Annual+Report+2018-2019.pdf

[14] So wurde in 37 Fällen der Einsatz einer Maßnahmen für nicht notwendig befunden; in 58 Fällen der Einsatz einer Maßnahme als unverhältnismäßig erachtet; in 48 Fällen befunden, dass der Zweck der Maßnahme auch mit weniger invasiven Mittel hätte erreicht werden können; in 68 Fälle befunden, dass dem Antrag für eine Maßnahme ausreichende Informationen über die relevante Tatsachen, nähere Umstände sowie Ausführungen

Ablehnungsentscheidungen und vermittelt der Öffentlichkeit so ein besseres Verständnis über seine Kontrolltätigkeit und deren Bedeutung. Der Kontrollrat sollte in zukünftigen Berichten in ähnlicher Weise dem Bundestag über seine Tätigkeit und Entscheidungsfindungen informieren.

Bisher sieht der Entwurf lediglich vor, dass der Unabhängige Kontrollrat unter sehr strengen Voraussetzungen in nicht näher bestimmter Weise dem Bundestag über Beanstandungen unterrichten kann. Die unnötig komplexe Verfahrensweise bei den Beanstandungen haben wir unter Punkt 2.3 in diesem Abschnitt A bereits erörtert.

Wie am niederländischen Beispiel verdeutlicht, ist es möglich ohne schützenswerte Informationen über den Auslandsnachrichtendienst und seine Arbeitsweisen preiszugeben. Wichtig wäre auch in den Berichten die Anzahl der Eilverfahren (§ 23 Abs. 4 Satz 2 und § 23 Abs. 7 Satz 3) mit dem standardmäßigen Genehmigungsverfahren (§ 23 Abs. 4 Satz 1 und § 23 Abs. 7 Satz 1) in Bezug zu setzen, um zu sehen, wie häufig in der Praxis von der Regel abgewichen wurde. Zudem sollten die Berichte über die Einbindung des Kontrollrats in die hoffentlich weiter wachsende Kontroll-Kooperation europäischer Aufsichtsgremien informieren.

3. 7. Evaluierung

Trotz der bereits genannten und verbesserungswürdigen Berichtspflichten werden viele Schritte der Rechtskontrolle "Parlament und Öffentlichkeit weithin verschlossen bleiben" (BVerfGE 1 BvR 2835/17; Rn. 299). Umso wichtiger ist es daher, “die Effektivität sowohl der Kontrolle in der Praxis als auch der gesetzlichen Regelungen in regelmäßigen Abständen zu evaluieren” (BVerfGE 1 BvR 2835/17, Rn 299). Eine Evaluierungspflicht ist als Kompensation für den eingeschränkten Rechtsschutz vonnöten, zumal sich “die Bedingungen der Überwachungsmaßnahmen wie deren Kontrolle angesichts der Fortentwicklung der Technik schnell wandeln können” (BVerfGE 1 BvR 2835/17, Rn 299).

Bei der im Entwurf in § 61 eröffneten Möglichkeit, alle fünf Jahre “die Wirksamkeit der Kontrolle fortlaufend (zu) überprüfen (Begründungstext, S. 129) bezieht sich aber leider nur auf die §§ 40 bis 58. Dabei wäre es wichtig, auch die Erfahrungen in der Zusammenarbeit mit dem Kanzleramt und dem BND im Rahmen der Anordnungsprozesse zum Gegenstand der Evaluationen zu machen. Zudem ist nicht ersichtlich, warum die beamteten, sicherheitsüberprüften (§ 53) und auf Lebenszeit zur Geheimhaltung verpflichteten (§ 54) Mitarbeiter:innen des Unabhängigen Kontrollrats nicht auch zumindest in Teilen in die Evaluation gemäß § 27 eingebunden werden sollen. Unabhängig von der nicht zur Zuständigkeit des Unabhängigen Kontrollrats gehörenden Prüfung der Zweckmäßigkeit von Überwachungsmaßnahmen, gibt es dennoch viele Informationen, die für die Ausübung der Rechtsmäßigkeitsprüfungen essentiell wären.

Hier wäre auch darüber nachzudenken, ob der Unabhängige Kontrollrat bei dieser wichtigen Berichtspflicht nicht auch den Bundestag und auch die Öffentlichkeit direkt informieren

---

über technische Risiken fehlten; in 26 Fällen entschieden, dass eine unzureichende rechtliche Grundlage für die beantragte Maßnahme vorlag; in 21 Fällen entschieden, dass eine beantragte Maßnahme den Geltungsbereich des Gesetzes überschritten hatte.

könnte – vielleicht in Ergänzung zum eingestuften Bericht an das PKGr. Das erscheint uns, gerade mit Blick auf die fehlende Möglichkeit den Stand von Wissenschaft und Technik im Rahmen eines Beirats regelmäßig einzuholen, als eine notwendige Ergänzung.

3. 8. Geheimhaltung

Vor dem Hintergrund, dass alle Mitarbeiter:innen des Unabhängigen Kontrollrats sicherheitsüberprüft sein sollen, und dass das Kontrollorgan “in den hoch sensiblen Bereich der Informationen ausländischer Nachrichtendienste Einsicht nehmen kann” (S. 113), verwundert die mysteriös anmutende Ausnahmesituation im Begründungstext zu § 56 Abs. 3 (S. 126): "In diesem Zusammenhang ist eine entsprechende Ausnahmesituation, die nur eine Unterrichtung eines sehr engen Personenkreises ermöglicht, nicht gänzlich auszuschließen. In einem solchen Fall wird das Bundeskanzleramt die Entscheidung gegenüber dem Unabhängigen Kontrollrat begründen müssen und gemeinsam nach einer angemessenen Unterrichtungsmöglichkeit suchen, die trotz der Aunsnahmesituation die erforderliche Rechtskontrolle ermöglicht." Uns ist nicht klar, was das für ein Fall sein könnte und uns erscheint, dass es präzisere Vorgaben für diese “Unterrrichtungsmöglichkeit” bedarf.

3.9. Synergien bei der Evaluation von Rechtmäßigkeit und Geeignetheit

Der Unabhängige Kontrollrat sollte nicht nur an der Evaluation der Kontrolltätigkeit (gem. § 61), sondern auch bei der entscheidenden Frage der Erforderlichkeit, also z.B. ob die Erhebung der Daten den Zweck erfüllt hat und welche Optimierungsschritte bei der Datenverarbeitung nötig sind, beteiligt werden. Der BND hat laut Entwurf unverzüglich und danach spätestens alle sieben Jahre zu prüfen, ob die mit Suchbegriffen erhobenen Inhalte "allein oder zusammen mit bereits vorliegenden Daten" für die Zwecke der strategischen Ausland-Fernmeldeaufklärung erforderlich sind (§ 27 Abs. 1).

Hierbei ist zu bedenken, dass die höchstrichterliche Entscheidung zum BND-Gesetz ein Mindestmaß an Änderungen im Sinne der Vereinbarkeit des strategischen Ausland-Fernmeldeaufklärung mit dem Grundgesetz skizziert hat. Weil es sich dabei allein auf die Rechtmäßigkeitsprüfung bezogen hat, heisst nicht, dass es dem Gesetzgeber nicht möglich wäre, auch eine Einbindung des Unabhängigen Kontrollrats bei der Zweckmäßigkeitsprüfung zu ermögliche. Wir glauben, dass man hier weitergehen sollte und über das im Urteil geforderte Minimum mehr Kontrolle wagen sollte.

→ **bessere Praxis:** Aufsichtsbehörden wie das belgische Comiteri[15] oder die schweizer Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten[16] haben zum Beispiel einen expliziten Auftrag auch die Zweckmässigkeit und Wirksamkeit der Nachrichtendienste zu prüfen. Diese sollte zumindest nach einer gewissen Einarbeitungsphase in die umfassenden Tätigkeiten der Rechtmäßigkeitsprüfung zukünftig ebenso dem Unabhängigen Kontrollrat zufallen, der als unabhängige und gleichwohl sachkundige Stimme die Evaluation der technischen Aufklärung unterstützen kann. Für die Mitarbeiter:innen des Kontrollrats würden ja ohnehin strengste Geheimhaltungs- und Aussagevorgaben gelten.

[15] Siehe https://www.comiteri.be/index.php/en/
[16] Siehe https://www.ab-nd.admin.ch/de/die-organisation-der-ab-nd/aufgaben.html

B. Kritik an der Ausgestaltung der Überwachungsbefugnisse und der Datenverarbeitung

1. Einleitung

Im Zuge der weiteren gesetzgeberischen Arbeit an der Novellierung des BND-Gesetzes sollte der Bundestag innehalten und sich fragen, ob die Praxis der Ausland-Ausland Fernmeldeaufklärung, so wie sie in den Randnummern 15 ff des Urteils beschrieben wurde, nicht mit europäischer Rechtssprechung in Konflikt geraten könnte. Klar ist zwar, dass die Ausland-Ausland Fernmeldeaufklärung grundsätzlich vom Bundesverfassungsgericht als verfassungskonformes Instrument der Sicherheitsvorsorge legitimiert wurde. Bei dem jetzt vorliegenden Entwurf könnten allerdings zu viele Vorgaben enthalten sein, die denen ähneln, die der Europäische Gerichtshof (EUGH) in der Schrems II Entscheidung gegenüber dem U.S. Nachrichtendienstrecht oder in der Privacy International Entscheidung vom 6. Oktober 2020 (C-623/17) mit Blick auf das britische Nachrichtendienstrecht als ungerechtfertigt moniert hat. Nach Ansicht des EUGH überschreiten sie “die Grenzen dessen [...], was in einer demokratischen Gesellschaft unbedingt notwendig ist”.

Im Folgenden fällt unser Augenmerk insbesondere auf die unbestimmten und mit der jüngeren europäischen Rechtsprechung nur schwer in Einklang zu bringenden Regelungen der Eignungsprüfung (Probebohrung) gemäß § 24. Sie öffnet unserer Meinung nach unter Ausschluss der Rechtskontrolle Tür und Tor für ein Übermaß an Datenerhebung.

2. Kritische Anmerkungen zur Eignungsprüfung (§ 24) im Lichte europäischer Rechtsprechung

Die Eignungsprüfung (§ 24) ist für den Bundesnachrichtendienst eine zentrale Befugnis. Hier geht es um die Wahrung der sogenannten “Kaltstartfähigkeit des BND”. Entgegen der Regel in § 19 Abs. 5 bekommt der Dienst gemäß § 24 die Erlaubnis personenbezogene Daten auch ohne vorherigen Einsatz von Suchbegriffen zu erheben.

Diese Regel ist aus vielerlei Hinsicht kritisch zu bewerten und bedarf unserer Meinung nach entscheidender Verbesserungen. Zudem sollte die Praxis vollumfänglich der Rechtskontrolle durch das administrative Kontrollorgan unterliegen, die bisher gänzlich außen vor bleibt. Auch gilt zu bedenken, dass mit dem Verweis auf die Legaldefinition der strategischen Ausland-Fernmeldeaufklärung (§ 19 Abs. 1) hier nur die Inhaltsdaten gemeint sind. Die Verkehrsdaten unterliegen damit ebensowenig der ohnehin nicht strengen Begrenzung des § 24 Abs. 1. Im Sinne der Rechtsklarheit ist die Aussage in § 19 Abs. 5, wonach "personenbezogene Inhaltsdaten im Rahmen der strategischen Ausland-Fernmeldeaufklärung nur anhand von Suchbegriffen" erhoben werden dürfen so nicht haltbar. Man sollte deshalb zumindest in § 19 Abs. 5 um einen 3. Satz ergänzen: "Für weitreichende Ausnahmen siehe die Bestimmungen in § 24 Abs. 1 und § 24 Abs. 7."

2. 1. Eignungsprüfung beim Anordnungsverfahren berücksichtigen

→ **Bessere Praxis:** Neuseeland hat aufgrund der zentralen Bedeutung von sogenannten Probebohrungen zur Prüfung der Eignung von Telekommunikationsnetzen oder zur Bestimmung geeigneter Suchbegriffe eine wichtige Regel ins Nachrichtendienstrecht aufgenommen, mit der der Grundrechtsschutz auch bei der Eignungsprüfung besser gewahrt werden soll. Laut “Part 4 Authorisations - Subpart 3 - Practice Warrants - Section 91 - Application for issue of Practice Warrant” etabliert der Intelligence and Security Act 2017 ein detailliertes Genehmigungsverfahren unter Beteiligung des Chief Commissioner of Intelligence Warrants und des Inspector General.[17]

2. 2. Unbestimmte Verlängerung der Eignungsprüfung gemäß § 24 Abs. 2

Laut Referentenentwurf darf die Eignungsprüfung mehrmalig um jeweils sechs Monate verlängert werden. Das ist viel zu unbestimmt. Hier könnte der BND durch Ketten-Verlängerungen einen bedeutenden Teil seiner technischen Aufklärung, die laut Grundsatzurteil aus Karlsruhe in vielerlei Hinsicht begrenzt und wirksamer unabhängig kontrolliert werden sollte, über die Eignungsprüfung laufen lassen und somit der Rechtskontrolle und dem Wirkungsbereich zahlreicher Schutznormen im BND-Gesetz entziehen.

Im Interesse der Rechtsklarheit sollte in § 19 Abs. 5 ein Verweis auf die Ausnahmetatbestände in § 24 geschaffen werden. Zudem sollte die Rechtmäßigkeitsprüfung der Maßnahmen nach § 24 in die Zuständigkeitskataloge der gerichtsähnlichen und administrativen Kontrollorgane (§ 42 und § 51, respektive) aufgenommen werden. Dementsprechend sollte § 24 Abs. 6 geändert werden, sodass die Löschprotokolle der im Rahmen der Eignungsprüfung erhobenen Daten nicht nur für die dienstinterne Kontrolle der Datenverarbeitung zur Verfügung stehen, sondern auch für die administrative Rechtskontrolle nutzbar gemacht werden können. Hier wäre es zudem wichtig, dass die im Rahmen der Eignungsprüfung erhobenen, verarbeiteten und übermittelten Daten (§ 24 Abs. 7 Nr. 2; siehe dazu auch die Anmerkungen im Abschnitt C dieser Stellungnahme) auch bei den Evaluationen nach § 27 und § 61 und den daraus resultierenden Berichten berücksichtigt werden.

2. 3. Kritik an der Bestimmung, Unternehmen zur Datenausleitung im Rahmen der Eignungsprüfung zu verpflichten

Gemäß § 24 Abs. 4 können Anbieter von Telekommunikationsdiensten zur Datenausleitung im Rahmen der Eignungsprüfung verpflichtet werden. Hier ist festzustellen, dass die Datenerhebung im Rahmen der Eignungsprüfung sowohl mit Blick auf die zeitliche Begrenzung aber auch auf die Erfassungsvolumina keiner strengen Begrenzung unterliegt. Dies, und die fehlende Beteiligung der Rechtskontrolle an der Praxis der Eignungsprüfung, ist an der Regelung in der jetzigen Form deutlich zu kritisieren. Zudem bestehen erhebliche Zweifel, ob diese Regel mit der jüngeren europäischen Rechtsprechung im Einklang steht.

[17] Siehe http://www.legislation.govt.nz/act/public/2017/0010/latest/whole.html#DLM7118938

Wir verweisen hier insbesondere auf die Privacy International Entscheidung des Europäischen Gerichtshofs (EUGH) vom 6. Oktober dieses Jahres.[18]

Wenn man die Argumente der Urteilsbegründung des EUGH (siehe die einschlägigen Randnummern 78-81; zur Zeit noch nicht in deutscher Sprache übersetzt) auf die Änderungen des Referentenentwurfs am BND-Gesetz anwendet, so müsste man unserer Meinung nach ebenso zum Ergebnis kommen, dass die vorgesehene Vorschrift gemäß § 24 Abs. 4 nicht haltbar ist. Sie ist unserer Meinung ebenso "ungerechtfertigt, weil sie die Grenzen dessen überschreitet, was in einer demokratischen Gesellschaft unbedingt notwendig ist".

> […] "national legislation governing access to traffic data and location data must rely on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data at issue (see, to that effect, judgment of 21 December 2016, *Tele2*, C‑203/15 and C‑698/15, EU:C:2016:970, paragraph 119 and the case-law cited).
>
> Those requirements apply, a fortiori, to a legislative measure, such as that at issue in the main proceedings, on the basis of which the competent national authority *may require providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission.* Such transmission has the effect of making that data available to the public authorities (see, by analogy, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 212).
>
> Given that the transmission of traffic data and location data is carried out in a general and indiscriminate way, it is comprehensive in that it affects all persons using electronic communications services. It therefore applies even to persons for whom there is no evidence to suggest that their conduct might have a link, even an indirect or remote one, with the objective of safeguarding national security and, in particular, without any relationship being established between the data which is to be transmitted and a threat to national security (see, to that effect, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C‑293/12 and C‑594/12, EU:C:2014:238, paragraphs 57 and 58, and of 21 December 2016, *Tele2*, C‑203/15 and C‑698/15, EU:C:2016:970, paragraph 105). Having regard to the fact that the transmission of such data to public authorities is equivalent, in accordance with the finding in paragraph 79 above, to access, it must be held that legislation which permits the general and indiscriminate transmission of data to public authorities entails general access.
>
> It follows that national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter.

3. Schwächen bei Filter-Technik und Datenkennzeichnung

3. 1. Filter nach Stand der Wissenschaft und Technik

Anders als vom Bundesverfassungsgericht in Rn. 173 verlangt ("Der Dienst ist darauf zu verpflichten, die Filtermethoden kontinuierlich fortzuentwickeln und auf dem Stand von

[18] Siehe http://curia.europa.eu/juris/document/document.jsf;jsessionid=CFAA160AC259FF995ABBB73585790AD5?text=&docid=232083&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8422287 -- zur Zeit nicht auf Deutsch abrufbar.

Wissenschaft und Technik zu halten"), sieht der Gesetzentwurf in § 19 Abs. 7 lediglich vor, dass die Filtermethoden kontinuierlich weiterentwickelt und auf dem Stand der Technik zu halten sind. Das ist ein deutlicher Unterschied, denn der Stand von *Wissenschaft und Technik* ist ein besserer Garant für den Grundrechtsschutz als der lediglich von der Exekutive nicht weiter festzulegender Stand der Technik. Hier erfüllt der Referentenentwurf nicht die Vorgaben aus Karlsruhe.

3. 2. Keine Anreize zur Nutzung von G10-Verkehren setzen

Es ist grundsätzlich zu begrüßen, dass fälschlicherweise nicht herausgefilterte G10-Verkehre unverzüglich und automatisiert gelöscht werden müssen (nach § 19 Abs. 7). Die dann folgende Ausnahme, dass die Löschung nicht erfolgen muss, "wenn tatsächliche Anhaltspunkte dafür vorliegen, dass durch die Weiterverarbeitung der Daten eine erhebliche Gefahr [...] abgewendet werden kann" läuft der wichtigen Grundprämisse der schnellen, automatischen Löschung zuwider. Wenn die Löschung automatisiert erfolgt, stellt sich die Frage, wie die unzulässig erhobenen G10-Verkehre dennoch auf diese Ausnahme hin geprüft werden können. Dafür müssen diese Daten erst weiter verarbeitet anstatt wie vorgegeben unverzüglich gelöscht werden, was darauf hindeutet, dass die Löschung nicht in jedem Fall automatisiert abläuft oder erst nach einer Zwischenauswertung greift. Um Vertrauen in die Rechtmäßigkeit der Datenfilterung zu schaffen, sollten all diese Anreize ausgeschlossen werden,entgegen der eindeutigen Vorgabe aus § 19 Abs. 7 Satz 1 dennoch Daten von Inländern zu erfassen und auszuwerten.

→ **Bessere Praxis:** Die Genauigkeit und damit verbundene Verhältnismäßigkeit der Filtersysteme in der strategischen Aufklärung wird immer wieder in Zweifel gezogen. Auch kleine Fehlerquoten können bei großen Datenmengen signifikante Grundrechtseingriffe verursachen. Eine Rechtsgrundlage für die unabhängige Auditierung der Filter würde helfen, diese Zweifel auszuräumen. Das niederländische unabhängige Aufsichtsgremium CTIVD hat 2019 einen Bericht über den Einsatz von Filtern durch die niederländischen Dienste AIVD und MIVD veröffentlicht.[19] Eine solche Prüfkompetenz für Filter könnte auch dem Unabhängigen Kontrollrat übertragen werden.

3. 3. Kennzeichnung von Verkehrs- und Metadaten

Der BND darf laut Entwurf personenbezogene Verkehrsdaten verarbeiten (§ 26 Abs. 1), was laut Begründung auch "alle weiteren personenbezogenen Metadaten" umfasst (S. 82). "Die Erhebung von personenbezogenen Verkehrs- und Metadaten, die nicht im Zusammenhang mit einer Individualkommunikation stehen", so die Begründung, greife "mangels unmittelbaren Bezugs zu einer Telekommunikation im Sinne des Art. 10 GG lediglich in das Recht auf informationelle Selbstbestimmung des Betroffenen ein. Da es sich hierbei im Vergleich zum Fernmeldegeheimnis des Artikels 10 GG um ein niederschwelligeres Grundrecht handelt, ist die Erhebung solcher Metadaten auf Grundlage dieser Norm erst recht möglich" (Begründungstext, S. 82).

Dieser Logik ist entschieden zu widersprechen: Erstens ist unklar warum das Recht auf informationelle Selbstbestimmung als niedrigschwelliger anzusehen sein sollte. Gerade in der digitalisierten Welt kommt diesem Grundrecht eine wachsende Bedeutung zu. Zweitens

[19] CTIVD, "Progress Report", 17. Juli 2019 (CTIVD Nr. 63), https://www.ctivd.nl/documenten/rapporten/2019/09/03/index

darf man nicht außer Acht lassen, dass, je nach Kontext der Datenerhebung, auch eine Reihe weiterer Grundrechte berührt sein könnten, wie die Pressefreiheit (Art 5 GG) etwa bei Erfassung von Metadaten von Redaktionsnetzwerken oder die Unverletzbarkeit der Wohnung (Art 13 GG) etwa wenn auf Daten von Smart-Home-Anbietern oder Cloud-Plattformen für Vernetzte Endgeräte zugegriffen wird.

Selbst wenn bestimmte Metadaten nicht direkt einer konkreten Individualkommunikation zuzuordnen sind, können sie im Zeitverlauf und in der Auswertung mit anderen Daten extrem viel über eine Person oder Gruppe aussagen und damit Grundrechtsrelevanz entfalten. Außerdem ignoriert die Begründung den gesamtgesellschaftlichen Vertrauensverlust und den Abschreckungseffekt von solchen unbegrenzten Metadatenerfassungen, zum Beispiel auf die Ausübung der Versammlungsfreiheit (Art 8 GG) oder der Vereinigungsfreiheit (Art 9 GG).

Daher sollten auch Verkehrs- bzw. Metadaten zur Sicherstellung einer rechtmäßigen Verarbeitung stets gekennzeichnet werden und nicht erst "im Rahmen der manuellen Auswertung" (§ 26 Abs. 2). Hinsichtlich der enorm großen Volumen an Metadaten bei der technischen Aufklärung scheint eine manuelle Kennzeichnung mehr als unrealistisch und nicht zweckmäßig. Die Kennzeichnung sollte daher, einheitlich zu den anderen Kennzeichnungsvorgaben, direkt bei der Erfassung automatisiert erfolgen, mindestens unter Angabe von Rechtsgrundlage und Erfassungsmethode.

Die Logik, dass Verkehrsdaten, die nicht durch einen (menschlichen) Kommunikationsvorgang entstehen, weniger (Grundrechts-) Schutz genießen, greift ebenso mit Blick auf die Ausnahmen für "Maschine-zu-Maschine-Kommunikation" (§ 26 Abs 3 Satz 2) zu kurz. Darunter könnten etwa Ortungsdaten, Funkzellendaten, Daten von Fitness Trackern, und Banktransaktionsdaten von Inländern fallen. Solche Verkehrdatenüberwachung stellt keine "Erhebung von Sachdaten, die mangels Grundrechtsrelevanz keiner Regelung bedürfen" (S. 57) dar. Der Raum für divergierende Rechtsauslegungen bei der Erhebung von Metadaten sollte unserer Meinung nach ausgeräumt werden.

→ **Bessere Praxis:** Ein Ansatzpunkt bietet dafür das niederländische Nachrichtendienstrecht. Es hat die Unterscheidung zwischen Verkehrs- und Inhaltsdaten, beziehungsweise personenbezogenen Daten und Sach- oder Metadaten gänzlich verworfen. Es verwendet stattdessen einheitliche Schutzvorschriften für alle Datenarten, da die Trennung und Kennzeichnung in der strategischen Aufklärung in den meisten Fällen nicht zuverlässig gelingen kann.

3. 4. Auch Kennzeichnung bei Übermittlung

Die grundsätzliche Verpflichtung, personenbezogene Daten unmittelbar nach der Erhebung unter Angabe des Zwecks und des Mittels der Datenerhebung zu kennzeichnen, enthält eine Generalausnahme für Übermittlungen (§ 19 Abs. 10). Einerseits ist diese bei Übermittlungen ins Ausland nachvollziehbar, um die Offenlegung der technischen Leistungsfähigkeit des BNDs zu verhindern. Bei der Übermittlung an inländische Behörden überzeugt dieses Argument jedoch nicht, die Kennzeichnung sollte dort zur Ermöglichung der Rückverfolgung der Datenherkunft festgeschrieben werden.

Die zu kennzeichnenden Informationen ließen sich zudem ohne Probleme ausweiten. Die Angabe von Zweck und Erhebungsmethode ist ein guter Anfang, mit Blick auf die Kontrolle (der die Kennzeichnung insbesondere dienen soll, laut S. 70 der Gesetzesbegründung) sollten die erhobenen Daten aber noch detaillierter gekennzeichnet werden. In Betracht kommt zum Beispiel eine genauere Kennzeichnung der Datenherkunft und der zulässigen Auswertungsmethoden. Hier ist insbesondere auf die Erfordernisse der administrativen Rechtskontrolle einzugehen, um die Datenhandhabung des BND für diese effizient nachverfolgbar zu machen.

→ **Bessere Praxis:** Der französische Gesetzgeber hat verbindliche Vorab-Gutachten der Aufsichtsbehörde für Datenkennzeichnungsregeln gesetzlich verankert. In der Vergangenheit beinhalteten diese Stellungnahmen der CNCTR zum Beispiel Anforderungen zur Erfassung von Verkehrsdaten, Speicherfristen, Speicherbedingungen und zur Erstellung von Log-Dateien.[20] Eine solche verpflichtende Stellungnahme würde auch der administrativen Rechtskontrolle zugutekommen.

C. Bessere rechtsstaatliche Einhegung und Kontrolle mit Bezug auf die privilegierte Zusammenarbeit des BND mit der Bundeswehr

1. Einleitung

Im Zuge der Novellierung des BND-Gesetzes wird die Zusammenarbeit des Bundesnachrichtendienstes mit der Bundeswehr, beziehungsweise mit “Dienststellen im Geschäftsbereich des Bundesministeriums der Verteidigung” (siehe § 12 Abs. 1), deutlich stärker hervorgehoben als in der bisherigen Gesetzesfassung. So werden im Referentenentwurf neue Grundlagen für den Datentransfer im Rahmen der “privilegierten Zusammenarbeit” geschaffen (§ 24 Abs. 7 Nr. 2) bzw. werden bestehende Befugnisse des BNDs, wie das Teilen von Erkenntnissen im Rahmen von projektbezogenen gemeinsamen Dateien mit inländischen öffentlichen Stellen, nunmehr auch für die Zusammenarbeit des BNDs mit der Bundeswehr möglich gemacht. Zudem wird auch die automatisierte Übermittlung von personenbezogenen Daten an die Bundeswehr, die aus der strategischen Ausland-Fernmeldeaufklärung mit dem Zweck der Gefahrenfrüherkennung erhoben wurden, gemäß § 29 Abs. 5 neu geregelt.

Bei den folgenden Bemerkungen geht es nicht um die Legitimation der Bundeswehr oder des Auslandsnachrichtendienstes als solche, sondern um die wichtige Frage, ob die zahlreichen und tief in die Grundrechte eingreifenden Überwachungsbefugnisse, die Datenübermittlungen und die Datenverarbeitung ausreichend rechtsstaatlich begrenzt werden und ob über das gesamte Spektrum des exekutiven Handelns eine ausreichende Rechtskontrolle besteht oder ob es wichtige Kontrollvakuuen zu adressieren gilt.

[20] Wetzling und Vieth, "Massenüberwachung bändigen: Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich", 2018, S. 70, https://www.stiftung-nv.de/sites/default/files/massenuberwachung_bandigen_-_web.pdf

Unserer Meinung nach stehen hier leider zu viele offene Fragen im Raum. Aufgrund gänzlich unterschiedlicher Kontrolldichten beim Bundesnachrichtendienst (bei reformierter Gesetzesgrundlage im Vergleich zur Bundeswehr deutlich höher) und der Bundeswehr (bei aktuellem Gesetzesstand im Vergleich zum Bundesnachrichtendienst deutlich geringer) besteht die Gefahr, dass Datenübermittlungen beispielsweise vom BND zu Dienststellen im Geschäftsbereich des Bundesministeriums der Verteidigung bewusst durchgeführt werden, um die weitere Datenverarbeitung einer geringeren Kontrolldichte auszusetzen. Die Möglichkeit eines derartigen inländischen Ringtausches könnte durch bessere Kontrollvorgaben begrenzt werden. Daher haben wir in diesem Abschnitt einige erste Empfehlungen für den Gesetzgeber ausgesprochen, was im Rahmen dieser Gesetzgebung – aber letztlich auch im Rahmen einer Reform des Rechts des militärischen Nachrichtendienstwesens angegangen werden müsste.

2. Anmerkungen zu § 12 und § 24 des Referentenentwurfs

2. 1. Projektbezogene gemeinsame Dateien werden auf Dienststellen im Geschäftsbereich des BMVg erweitert (§ 12 Abs. 1)

Im Begründungstext wird darauf verwiesen, dass die bisherige Befugnis des BND zum Zwecke des Austausches und der gemeinsamen Auswertung von Erkenntnissen projektbezogene Dateien mit inländischen Stellen einzurichten “an wenigen Stellen angepasst wurde” (S. 55). Mit Blick auf die vage Bezeichnung “Dienststellen im Geschäftsbereich des BMVg” erscheint das als eine Erweiterung von entscheidender Tragweite, gerade auch mit Blick auf die im folgenden angesprochenen Fragen der Schutznormen und der Rechtskontrolle.

Gemäß § 12 Abs. 3 soll eine Dateianordnung für projektbezogene gemeinsame Dateien, was eine entscheidende Voraussetzung für eine Datenverarbeitungs- und Datenschutzkontrolle darstellt, nur vom BND angelegt werden, wenn der BND die gemeinsame Datei auch führt (S. 55). Hier sollte im Sinne der Rechtsklarheit im § 12 Abs. 3 nach dem Wort “Datei” die Wörter “durch den Bundesnachrichtendienst” eingefügt werden. Das hat auch Relevanz für § 12 Abs. 6 (siehe unten).

Es stellen sich zentrale Fragen, auf die in der Begründung des Referentenentwurfs nicht oder zumindest nicht ausreichend eingegangen wird. Erstens, welche Regel gilt für Dateianordnungen im Sinne des § 8 BND-Gesetzes für projektbezogene Dateien, die nicht vom BND sondern von “Dienststellen im Geschäftsbereich der Bundeswehr” geführt werden? Hier sollten das Recht der Bundeswehr, gerade auch wegen der Auslandsgeltung von Art 10 GG, einen ähnlichen Passus enthalten wie die in §§ 6, 7 und 9 im Referentenentwurf angelegten Bestimmungen zur Speicherung und Veränderung und Nutzung; Berichtigung, Löschung und Verarbeitungseinschränkungen; sowie zu Auskünften an Betroffene. Zweitens sollte dringend der Frage nachgegangen werden, ob für die aus der Aufklärung durch das militärische Nachrichtendienstwesen gewonnenen Daten, sowie die aus dem “nicht kooperativen Zugang” der Einheiten des elektronischen Kampfs gewonnenen Daten, eine ausreichend verfassungskonforme Rechtsgrundlage für die Erhebung und Verarbeitung dieser Daten besteht und ob die Kontrolldichte nicht auch deutlich ausgeweitet werden sollte. Dies betrifft im Übrigen auch die in den Dienststellen im Geschäftsbereich des

Bundesministeriums für Verteidigung betriebene Verarbeitung der durch den BND übermittelten Daten.

In § 12 Abs. 6 sollte im Sinne des Bestimmtheitsgebots darauf hingewiesen werden, dass die Verpflichtung eine detaillierte Dateianordnung anzulegen nur für einen Teil der projektbezogenen Dateien gilt, nämlich nur für diese, die der BND selbst führt. Ob im Sinne des § 12 Abs. 6 Satz 2 schließlich die jeweils zuständige Fachaufsicht der zusammenarbeitenden Behörden einer Dateianordnung zustimmt, und ob im Sinne des § 12 Abs. 6 Satz 3, der oder die BfDI vor Erlass einer Dateianordnung anzuhören ist, hängt ebenfalls davon ab, ob die Behörde, die eine projektbezogene Datei führt überhaupt per Gesetz dazu verpflichtet ist, eine Dateianordnung im Sinne des § 12 Abs. 6 zu führen. Falls es hier Lücken gibt, sprich einige Behörden keine gesetzliche Verpflichtung haben, eine Dateianordnung zu führen, könnte man aus Sicht des BND vermutlich durch das Nichtführen (z.B. wenn die Dateiführung bei der Bundeswehr liegt) einer projektbezogenen gemeinsamen Datei die Schutzbestimmungen des § 12 Abs. 6 Satz 2 und Satz 3 umgehen.

2. 2. Zweckänderung bei im Rahmen der Eignungsprüfung erhobenen Daten (§ 24 Abs. 7)

Im Rahmen der privilegierten Zusammenarbeit zwischen BND und Bundeswehr wird im vorliegenden Gesetzentwurf die ohnehin schon unzureichend gefasste Ausnahme vom Grundsatz in § 19 Abs. 5 Satz 1 (der BND darf die Erhebung von personenbezogenen Inhaltsdaten nur anhand von Suchbegriffen durchführen), die die Eignungsprüfung nach § 24 ja darstellt, um eine weitere Ausnahme vom Grundsatz gemäß § 24 Abs. 5 Satz 1 (im Rahmen der Eignungsprüfung erhobenen personenbezogenen Daten dürfen nur zum Zweck der Eignungsprüfung verwendet werden) verwässert. Gemäß § 24 Abs. 7 Nr. 2 soll die Übermittlung der im Rahmen der Eignungsprüfung erhobenen personenbezogenen Daten an die Bundeswehr, auch automatisiert und ohne Kennzeichnungspflicht beim BND möglich sein.

Natürlich sollen die im Rahmen eines durch den Bundestag legitimierten Bundeswehreinsatzes entsandten Soldatinnen und Soldaten umfassend von den Informationen des BND profitieren. Allerdings wird hier eine Befugnis geschaffen, wonach der BND ohne Suchbegriffe personenbezogene Inhalts-, Verkehrs- und sonstigen Metadaten im Rahmen der Eignungsprüfung automatisiert an die Bundeswehr weiterleiten kann. Über folgende Fragen sollte debattiert werden: Erstens, ist diese Befugnis sinnvoll und die Zweckänderung ausreichend begründet und verfassungskonform? In der Begründung steht, dass diese Form der zweckgeänderten Übermittlung an die Bundeswehr durch die in § 24 Abs. 7 Nr. 2 genannte Zwecke “streng begrenzt” ist. Dem würden wir widersprechen. Für die auch automatisiert möglichen Übermittlungen gelten nach jetziger Fassung keine Volumenbeschränkung und diese Maßnahmen könnten auch unbegrenzt oft für die Dauer von sechs Monaten wiederholt werden. Diesen Fragen sollte man kritisch nachgehen und für ein besseres Vertrauen in die verhältnismäßige und verfassungskonforme Ausübung von Überwachungsbefugnissen würde es helfen, wenn die Standards einer unabhängigen und professionellen internen Datenverarbeitungskontrolle über die verschiedenen Tätigkeitsfelder der Sicherheitsvorsorge angeglichen werden.

→ **Bessere Praxis:** Hier gilt es zu bedenken, dass Art. 45d GG von der “nachrichtendienstlichen Tätigkeit des Bundes” spricht, § 1 PKGr-Gesetz lediglich auf die

Tätigkeit des BfV, MAD und BND abstellt. Dabei sind, je nach Auslegung des Begriffs “nachrichtendienstliche Tätigkeiten”, zahlreiche ebenso einschlägige Tätigkeiten außerhalb der drei Dienste des Bundes in den letzten Jahren hinzugekommen, die ebenfalls in die Grundrechte eingreifen und einer stärkeren Kontrolle unterliegen sollten. Die Bundeswehr verfügt beispielsweise im Organisationsbereich Cyber- und Informationsraum (CIR) über das Kommando Strategische Aufklärung (KSA). Dem KSA unterstellt ist beispielsweise die Fernmeldetruppe Elektronischer Kampfführung (EloKa), die sich wiederum in einzelne Bataillone unterteilt. Dort werden Fernmeldeauflärung, also die Erfassung und Auswertung fremder Fernmeldeverkehre (COMINT) und elektronische Aufklärung, also die Erfassung und Auswertung von Ortungs-, Leit-, Lenk- und Navigationssystemen im elektromagnetischen Spektrum zur Informationsgewinnung (ELINT) betrieben. Zudem verantworten die Bataillone der Eloka-Truppe den elektronischen Kampf (EW) mittels elektronischer Gegenmaßnahmen (ECM), elektronischer Schutzmaßnahmen (ECCM) und elektronischer Unterstützungsmaßnahmen (ESM).[21]

Bei der umfangreichen Reform des kanadischen Sicherheitsrechts ist man z.B. dazu übergegangen, sich bei der Kontrolle auf die Erhebung, Verarbeitung und Weitergabe von mit nachrichtendienstlichen Mitteln erhobenen Daten abzustellen, und dabei eine Vielzahl von Behörden in den Blick zu nehmen. Das Mandat der Aufsichtsbehörde wurde also funktional, entlang der zu kontrollierenden Tätigkeiten, nicht anhand von einzelnen Behörden definiert. Da auch in der Bundesrepublik immer mehr Sicherheitsbehörden eng miteinander zusammenarbeiten müssen um ihre Aufgaben zu erfüllen, wäre eine ganzheitliche Aufsicht über nachrichtendienstliche Tätigkeiten auch hier geboten.

Vor dem Hintergrund der weit gefassten Befugnis in § 24 Abs. 7 drängen sich aber noch weitere Fragen auf: Inwiefern unterliegt die Datenverarbeitung bei der Bundeswehr und bei den Dienststellen im Geschäftsbereich des BMVg einer unabhängigen administrativen Rechtskontrolle und hat der oder die BfDI zudem ausreichende Zugangsmöglichkeiten für die unabhängige Datenschutzkontrolle? Welche Vorgaben gelten bzgl. der Weiterverarbeitung und des Austauschs von im Rahmen der Eignungsprüfung erhobenen Daten mit ausländischen öffentlichen Stellen durch die Bundeswehr? Laut Begründungstext S. 81 ist eine Übermittlung auch an Streitkräfte der Mitgliedstaaten der EU, an Streitkräfte im NATO-Verbund und an Streitkräfte der Staaten, die der europäischen Freihandelsassoziation angehören, zulässig. Das ist ein sehr großer Empfängerkreis.

Fazit

Das im Mai gefällte BND-Urteil macht deutlich, dass die Reichweite und Intensität von Überwachung im Zuge der Digitalisierung eine völlig neue Dimension angenommen hat. Die demokratische Kontrolle der Überwachung konnte mit dieser Entwicklung nicht Schritt halten. Infolgedessen ist die Kontrolldichte gesunken und mit Blick auf die fortlaufend erweiterten nachrichtendienstlichen Tätigkeiten und aufgestockten finanziellen Mittel des Bundes aktuell stark reformbedürftig.

[21] Diese Informationen wurden diesen Quellen entnommen: https://de.wikipedia.org/wiki/Nachrichtengewinnung_und_Aufkl%C3%A4rung;

Die jetzt eingeleitete Reform bietet die Gelegenheit, den Bundesnachrichtendienst endlich verfassungskonformen Regelungen zu unterwerfen, die unserer vernetzten Welt gerecht werden. Zahlreiche Beispiele aus anderen Ländern belegen, dass sich Kontrollstrukturen und -verfahren unabhängiger, moderner, effektiver und transparenter aufstellen lassen, als dies in diesem Entwurf der Fall ist.

Der Umfang, die Kontrollziele und die Technologie, die im Rahmen der administrativen Rechtskontrolle zum Einsatz kommen soll, bleiben im Gesetzentwurf und in seiner Begründung deutlich zu unbestimmt. Zudem befürchten wir, dass die häufigen Abgrenzungen der originären Kontrollzuständigkeiten zwischen dem administrativen Kontrollorgan und dem gerichtsähnlichen Kontrollorgan, dem Ziel eines funktionalen Kontrollmandats (Ende-zu-Ende Kontrolle) entgegensteht. Auch tritt das administrative Kontrollorgan gegenüber dem Spruchkörper viel zu häufig zurück, wie zum Beispiel bei dem umständlichen und langwierigen Prozess der Beanstandungen.

Zudem werden in diesem Entwurf Doppelkontrollen der Datenverarbeitung durch den Bundesdatenschutzbeauftragten und den Unabhängigen Kontrollrat in Kauf genommen. Diest ist für den BND ineffizient und auch aus Kostengründen zu kritisieren. Wir sollten unnötige Parallelstrukturen vermeiden und die Erfahrung des oder der BfDI stärker im Rahmen der administrativen Rechtskontrolle einbinden.

Wir hoffen, dass die umstrittenen Befugnisse nach § 34 sowie die zahlreichen Änderungen mit Blick auf die Übermittlungsvorschriften §§ 30ff von den weiteren Stellungnahmen aufgegriffen werden. Wir haben uns auf die Rechtskontrolle konzentriert und zudem die Eignungsprüfung im Lichte europäischer Rechtsprechung kritisch besprochen. Zudem haben wir die privilegierte Partnerschaft des Bundesnachrichtendienstes mit den Dienststellen im Geschäftsbereich des Bundesministeriums der Verteidigung in den §§ 12 und 24 vor allem mit Blick auf die Schutznormen und Kontrollvorgaben hin kritisiert.