Juni 2020 · Thorsten Wetzling und Daniel Moßbrucker

BND-Reform, die Zweite

Vorschläge zur Neustrukturierung der Nachrichtendienst-Kontrolle

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Mit dem Urteil des Bundsverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung liegt die Reform des BND-Gesetzes aus dem Jahr 2016 in Trümmern. Es bedarf nun einer neuen, echten Reform von Nachrichtendienstrecht und -kontrolle. Karlsruhe hat schließlich grundlegende Defizite im Status quo ausgemacht, die den Anforderungen des Grundgesetzes bei Weitem nicht genügen. Der Gesetzgeber hat auch deshalb bis Ende 2021 Zeit bekommen, um die gesetzlichen Grundlagen nun umfassend an die spezifischen Herausforderungen nachrichtendienstlicher Tätigkeit im Zeitalter von Internationalisierung und Digitalisierung anzupassen. Aussagen von Kanzleramtsminister Helge Braun lassen jedoch vermuten, dass die Bundesregierung sich erneut einen schlanken Fuß machen will.

In diesem Papier präsentieren wir auf Grundlage des Urteils einen Entwurf für eine weitreichende Neuordnung der deutschen Nachrichtendienst-Kontrolle. Wir verfolgen dabei das Ziel einer Ende-zu-Ende-Kontrolle, also einer Kontrolle nachrichtendienstlicher Überwachung beginnend mit der Genehmigung der Datenerfassung über den gesamten Prozess der Datenverarbeitung hinweg bis hin zur Übermittlung ins In- und Ausland.

Im Kern schlagen wir vor, die bisher untertourige, fragmentierte und nicht ausreichend unabhängige Rechtskontrolle in einem neu zu gründenden gerichtsähnlichen Kontrollrat, zuständig für alle deutschen Nachrichtendienste, zu bündeln. G10-Kommission und Unabhängiges Gremium werden abgeschafft. Der Kontrollrat besteht aus einem unabhängigen Spruchkörper mit umfassenden Kontroll- und Vetorechten. In ihm gilt ein kontradiktorisches Verfahren, sodass neben den Ministerialbeamt:innen zum Beispiel auch “Anwält:innen der Bürger:innen” oder Advokat:innen besonders vor Überwachung zu schützender Berufsgruppen wie Journalist:innen in den Sitzungen vertreten sind und dort eine anderes Licht auf die beantragten Maßnahmen werfen können.

Der Kontrollrat steht im engen Austausch mit dem Bundesdatenschutzbeauftragten (BfDI), der die zentrale Instanz der administrativen Rechtskontrolle wird. Die Mitarbeiter:innen des BfDI prüfen, ob im Prozess der Datenerhebung, -verarbeitung und -übermittlung die rechtlichen Standards eingehalten werden. Das ist eine umfangreiche und technisch anspruchsvolle Kontrollpflicht, die einen umfassenden Zugang zu allen informationstechnischen Systemen und Datenbanken des BND voraussetzt. Der BfDI muss die gesamte Verarbeitung der im Rahmen der strategischen Fernmeldeauf-

klärung anfallenden personenbezogenen Daten prüfen, inklusive internationaler Kooperationen mit ausländischen Nachrichtendiensten.

Es entstünde ein Kontrollgefüge, das mit Parlamentarischen Kontrollgremium (PKGr), Kontrollrat und BfDI nur noch drei wesentliche Institutionen mit klaren Zuständigkeiten kennt. Die Kontrollrechte, der Datenzugang, die technologische Ausstattung sowie die Kooperation zwischen den Kontrollinstanzen wären deutlich ausgebaut, um eine nachhaltigere, wirksamere und umfassende Aufsicht der nachrichtendienstlichen Tätigkeiten des Bundes zu gewähren.

	Status Quo		**Vorschlag**
Rechtsgrundlage	Inland-Ausland-Fernmeldeaufklärung nach Artikel 10-Gesetz	Ausland-Ausland Fernmeldeaufklärung nach BND-Gesetz	BND-Gesetz mit identischen Standards für Inland-Ausland- sowie Ausland-Ausland-Fernmeldeaufklärung
Spruchkörper	G10-Kommission (eingeschränkt)	Unabhängiges Gremium (eingeschränkt)	Rat der deutschen Nachrichtendienst-kontrolle
Rechtskontrolle	?*	BfDI (eingeschränkt)	BfDI
politische & finanzielle Kontrolle	Parlamentarisches Kontrollgremium & Vertrauensgremium	Parlamentarisches Kontrollgremium & Vertrauensgremium	Parlamentarisches Kontrollgremium

* Hier hat die G10-Kommission eine Kontrollbefugnis für die administrative Rechtskontrolle. Ihr fehlen aber Expertise und Ressourcen dafür. Der BfDI bleibt außen vor.

Inhalt

I. Einleitung*

Die Bundesregierung wollte im Zuge der Erkenntnisse aus dem NSA-Untersuchungsausschuss eigentlich die massenhafte Überwachung des Internet- und Telefonverkehrs durch den Bundesnachrichtendienst rechtsstaatlich einhegen. Nach dem Karlsruher Urteil bedarf es nun aber einer grundlegenderen Reform von Nachrichtendienstrecht und Kontrolle, denn dem Grundsatzurteil des Bundesverfassungsgerichts zufolge verstoßen die aktuellen Regelungen zur sogenannten Ausland-Ausland-Fernmeldeaufklärung gegen das Grundgesetz. Zeit für die BND-Reform, die Zweite.

Die Diskussion um die Fernmeldeaufklärung ist mit dem Richterspruch nicht beendet, sondern sie beginnt jetzt erst. Das Gericht fordert umfassende Reformen, um die strategische Überwachung "erstmals im Lichte des Art. 10 Abs. 1 GG (zu) regeln und damit in neuartiger Weise rechtsstaatliche Grenzen und Kontrollen schaffen" (Rn. 330)[1] zu können. Das Urteil eröffnet damit die Chance, die vielen überalteten, reformbedürftigen Rechtsnormen und die fragmentierte Nachrichtendienst-Kontrolle in Deutschland zu reformieren. Dort liegt derzeit vieles im Argen: Neben dem BND-Gesetz gibt es unter anderem erheblichen Reformbedarf beim Artikel 10-Gesetz, beim Verfassungsschutzrecht und beim Mandat der Bundeswehr für die Auslandsaufklärung. Auch der Einsatz von Bundestrojanern als nachrichtendienstliches Mittel ist umstritten. Internationalisierung und Digitalisierung haben die Geheimdienstarbeit in den vergangenen Jahren grundlegend verändert, aber die zahlreichen Institutionen ihrer Kontrolle operieren mit unzureichender Kontrolldichte und -technik. Es braucht jetzt eine Abkehr vom Status Quo samt der, vom Bundesdatenschutzbeauftragten monierten, "unzureichend geklärten und mitunter gespaltenen Zuständigkeiten" (Rn. 51).

Die Anzeichen verdichten sich jedoch, dass die Bundesregierung wie schon 2016 nicht den Mut aufbringt, die Arbeit der Nachrichtendienste umfassend neu zu gestalten. Obwohl das Gericht eine großzügige Frist zur Überarbeitung bis Ende 2021 gegeben hat und die Umsetzung der gebotenen Änderungen über das BND-Gesetz hinausgehen, will Kanzleramtsminister Helge Braun schon zum Ende der parlamentarischen Sommerpause den Regierungsentwurf durchs Kabinett bringen und wird wohl nur das unbedingt notwendige im BND-Gesetz ändern – und somit die Chance verstreichen lassen, den gesamten Prozess der strategischen Fernmeldeaufklärung in einem Gesetz zu regeln und einer weniger fragmentierten Kontrolle zuzuführen.

** Diese Studie wurde von der Deutschen Forschungsgemeinschaft (DFG-Projektnummer 396819157) gefördert.*

1 Bei den Randnummern beziehen wir uns im Folgenden immer auf das Urteil des Bundesverfassungsgerichts vom 19. Mai 2020, Az. 1 BvR 2835/17.

In diesem Impulspapier wollen wir Ideen präsentieren, wie das Urteil mit einer grundlegenden Neujustierung der Geheimdienstkontrolle in Deutschland umzusetzen wäre. Die zentralen Vorschläge:

- Die bisher fragmentierte Rechtskontrolle der Nachrichtendienste durch die G10-Kommission und das Unabhängige Gremium wird zusammengefasst in nur einem Gremium, dem neu zu schaffenden Rat der deutschen Nachrichtendienst-Kontrolle. Er besteht aus einem gerichtsähnlichen, unabhängigen Spruchkörper mit umfassenden Kontroll- und Vetorechten. In ihm gilt ein kontradiktorisches Verfahren. Dieser neue Kontrollrat wird zuständig für alle Nachrichtendienste auf Bundesebene – Bundesnachrichtendienst, Bundesamt für Verfassungsschutz und Militärischer Abschirmdienst.
- Der Bundesdatenschutzbeauftragte (BfDI) wird zentrale Instanz der administrativen Rechtskontrolle. Der BfDI hat demnach "den gesamten Prozess der strategischen Überwachung auf seine Rechtmäßigkeit zu prüfen" (Rn. 276). Das ist eine umfangreiche und technisch anspruchsvolle Kontrollpflicht, die sich auf die gesamte Verarbeitung der im Rahmen der strategischen Fernmeldeaufklärung anfallenden personenbezogenen Daten erstreckt, inklusive internationaler Kooperationen mit ausländischen Nachrichtendiensten.
- Das Parlamentarische Kontrollgremium wird mit dem Vertrauensgremium zusammengelegt und übernimmt dessen Aufgaben der Finanzkontrolle.
- Es wird ein Beirat geschaffen, um dem Kontrollrat und dem Bundesdatenschutzbeauftragten sowohl in technischen, rechtlichen und anderen Fragen dauerhaft beratend zur Seite zu stehen. Dieses Gremium sollte auch mit Personen besetzt werden, die sich für den Schutz von durch Überwachung besonders gefährdeten Berufsgruppen einsetzen, wie etwa Journalist:innen oder Anwält:innen.
- Die Aufsicht würde professionalisiert, bekäme moderne Kontrolltechnologie, würde die Kontrolldichte erhöhen und würde extern beraten. Nur so kämen die Kontrolleur:innen erst in die Lage, die Nachrichtendienste mit ihren rund 13.000 Mitarbeitenden auf Bundesebene angemessen zu kontrollieren.

Ein solch grundlegender Neuentwurf ist jetzt vonnöten, um die zahlreichen und gehaltvollen Forderungen der Verfassungshüter politisch umzusetzen und dauerhaft für Rechtssicherheit und Rechtsstaatlichkeit zu sorgen.

Deutschland hat dank des Urteilsspruchs nun auch im internationalen Kontext eine neue Chance erhalten, glaubhafter in den Club demokratischer Länder einzutreten, die Nachrichtendienste wirksam kontrollieren. Dabei sind, auch das zeigen Vergleiche mit diesen Ländern, keine Einbußen bei der Sicherheitsvorsorge zu befürchten. Nach den Snowden-Veröffentlichungen hatte Deutschland gemeinsam mit Brasilien eine UN-Resolution 68/167 zu "The Right to Privacy in the Digital Age" eingebracht, in der sich die Bundesregierung verpflichtete, Massenüberwachung nur unter hohen Hürden und bei angemessener Kontrolle einzusetzen. Die anstehende Reform bietet die nächste Gelegenheit, den Versprechungen jetzt politische Taten folgen zu lassen.

II. Vorschlag für eine grundlegende Neustrukturierung der Kontroll-Architektur

Mit dem Karlsruher Grundsatz-Urteil ist endgültig geklärt, dass Artikel 10 des Grundgesetzes als Abwehrrecht für inländische wie ausländische Personen gleichermaßen gilt. Das Bundesverfassungsgericht folgte damit erwartungsgemäß der seit Jahren herrschenden Meinung in der juristischen Literatur, die von der Bundesregierung stets verneint wurde. Fortan kann die Ausland-Ausland-Fernmeldeaufklärung kein Instrument fernab des Grundgesetzes mehr sein, sondern muss wie alle anderen Überwachungsmaßnahmen deutscher Behörden auch an den Maßstäben des Telekommunikationsgeheimnisses gemessen werden.

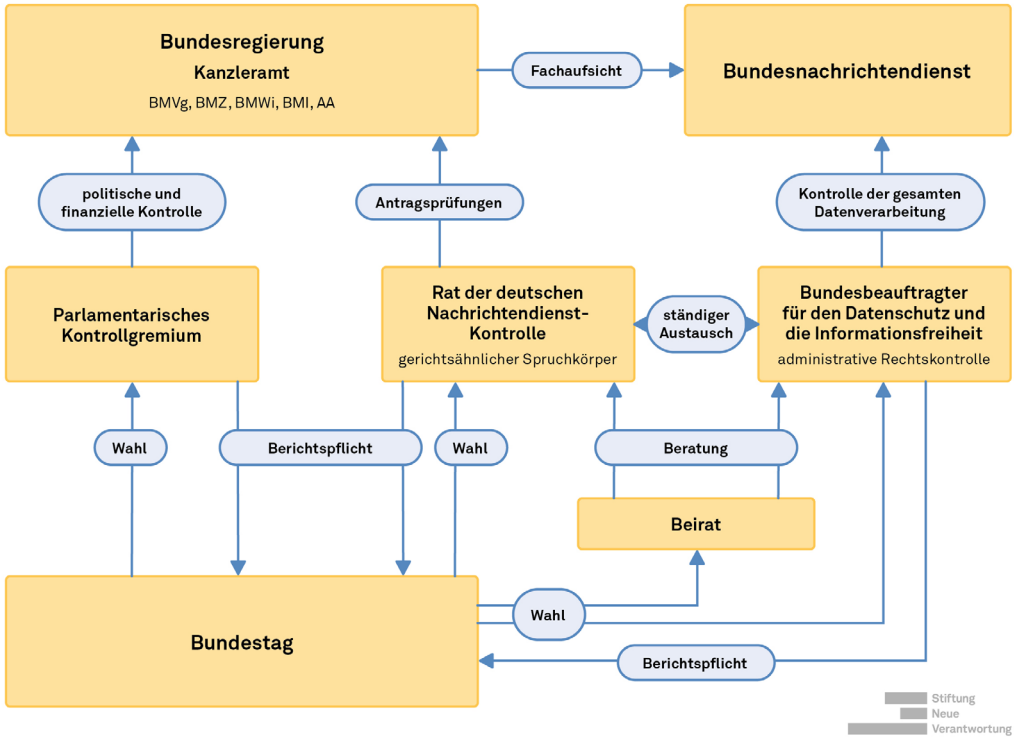
Zwar ist die strategische Fernmeldeaufklärung seit Jahrzehnten ein Instrument des BND, doch erst im Zuge des NSA-Untersuchungsausschusses des Bundestages hat eine breitere Öffentlichkeit in Deutschland von dieser Praxis erfahren. Anders als bei der gezielten Überwachung der Kommunikationsverkehre von bestimmten Personen oder Gruppen betrifft die strategische Fernmeldeaufklärung das allgemeine, verdachtsunabängige Überwachen von Kommunikationsströmen. Die Ausland-Ausland-Fernmeldeaufklärung nach dem BND-Gesetz ist, neben den sogenannten strategischen Beschränkungsmaßnahmen nach § 5 Artikel 10-Gesetz, ein wesentlicher Bereich dieser massenhaften Überwachung. Sie betrifft derzeit das Erfassen und Verarbeiten von täglich Billionen an Kommunikationsdaten, deren Ursprungs- und Endpunkt im Ausland liegen. Die Kommunikationsverkehre werden dabei in teil-automatisierten Prozessen mit Suchbegriffen gefiltert, um gegebenenfalls nachrichtendienstlich relevante Daten und Inhalte identifizieren zu können.

Wir schlagen nun vor, im Grundrechtsschutz nicht mehr anhand der Nationalität, sondern rein funktional zu unterscheiden. Entscheidend ist nicht die Herkunft der überwachten Menschen, sondern die Schwere des Grundrechtseingriffs und die Bedeutung für die Außen- und Sicherheitspolitik Deutschlands. Für die Kontrolle heißt dies, dass es nur noch ein gemeinsames Kontrollgefüge für die gesamte nachrichtendienstliche Überwachung geben kann: weg von einem fragmentierten, personell unterbesetzen Flickenteppich aus Kontrollgremien, hin zu einer schlanken Behörden-Organisationen mit ausreichend Personal und einschneidenden Kontrollrechten.

Unserem Vorschlag nach soll es – den Leitlinien des Karlsruher Urteils folgend – drei starke Institutionen geben, die Bundesregierung und Bun-

desnachrichtendienst kontrollieren. Während das Parlamentarische Kontrollgremium weiterhin für die politische Kontrolle verantwortlich bleibt, übernimmt es zudem die Aufgaben des abgeschafften Vertrauensgremiums. Neues Schwerpunkt-Organ der Rechtskontrolle wird ein neu zu schaffender Rat der deutschen Nachrichtendienst-Kontrolle (Kontrollrat). Dies ist ein vom parlamentarischen Kontrollgremium gewählter, gerichtsähnlicher Spruchkörper, der für den Grundrechtsschutz in der gesamten strategischen Fernmeldeaufklärung zuständig ist, inklusive der Datenverarbeitung bei internationalen Kooperationen. Die administrative Rechtskontrolle, also insbesondere die Einhaltung datenschutzrechtlicher Standards, übernimmt künftig vollständig der Bundesdatenschutzbeauftragte (BfDI). Kontrollrat und BfDI stehen im ständigen Austausch, um Kontrolllücken zu verhindern. Weder der Kontrollrat noch der BfDI werden in Zukunft als sogenannte Third-Party eingestuft. Sie können also auch umfassend die Kooperationen deutscher Dienste mit ausländischen Nachrichtendiensten kontrollieren.

In der Gesamtbetrachtung könnte ein neues institutionelles Gefüge für die Steuerung und Kontrolle der Fernmeldeaufklärung in Deutschland wie folgt aussehen:



Im Vergleich zum Status Quo wird die Durchschlagskraft der Kontrolle gestärkt durch

- eine deutliche Reduktion der Aufsichtsgremien durch den Wegfall des Unabhängigen Gremiums, des Vertrauensgremiums und der G10-Kommission, eine Professionalisierung der Rechtskontrolle mit der Gründung des Kontrollrats als alleinigen, gerichtsähnlichen Spruchkörper für die gesamte Fernmeldeaufklärung, und dem Bundesdatenschutzbeauftragten als Instanz der administrativen Rechtskontrolle mit umfassenderen Zugangsrechten und moderner Kontrolltechnik,
- eine deutlich erhöhte Kontrolldichte in allen Phasen der strategischen Überwachung von der Erhebung über die Verarbeitung bis hin zur Übermittlung im In- und Ausland,
- Informations- und Erfahrungsaustausch zwischen Kontrollrat und BfDI sowie einer häufigeren Konsultation mit dem PKGr,
- die Gründung eines Beirats, gewählt vom Bundestag und besetzt mit unabhängigen Expert:innen unterschiedlicher Fachrichtungen, zur Unterstützung der Rechtskontrolle, des Datenschutzes sowie der politischen Kontrolle durch PKGr und Parlament.

Die folgenden Kapitel erläutern und begründen unseren Vorschlag im Einzelnen. Wir beginnen mit einer Zusammenfassung der Prämisse, die diesem Vorschlag zugrunde liegt: eine Ende-zu-Ende-Kontrolle zur Wahrung eines umfassenden Grundrechtsschutzes (II.1). Es folgt eine nähere Beschreibung der Institutionen in unserem SIGINT-Governance Gefüge (II.2), ehe wir die von uns aus dem Karlsruher Urteil abgeleiteten Folgen für die Reform im Einzelnen diskutieren (Kapitel III & IV).

II.1 Prämisse: Ende-zu-Ende-Kontrolle

Die Verfassungsrichter haben in ihrem Urteil klargestellt, dass künftig die Rechtskontrolle über die gesamte strategische Fernmeldeaufklärung kein Desiderat mehr bleiben darf, sondern durch den Gesetzgeber bis spätestens Ende 2021 gesetzlich verankert und deutlich gestärkt werden muss. Kontrolllücken darf es nicht geben, wenn die Bundesregierung ein echtes Interesse an einem holistischen Grundrechtsschutz hat.

Wie drängend die Probleme sind, ist im Vorfeld der Urteilsfindung bekannt geworden. Beispielhaft sei genannt, dass viele der in Deutschland bis dato stark fragmentierten Aufsichtsgremien in der mündlichen Verhandlung beklagten, dass sie in der Praxis kaum bis gar keine Berührungspunkte mit-

einander hätten – und eine Ende-zu-Ende-Kontrolle nicht garantieren können, weil sie sich teilweise gar nicht austauschen dürfen. Dies betrifft insbesondere den Kontakt zwischen BfDI und dem Unabhängigen Gremium, welches gegenwärtig für Genehmigungen bei der Ausland-Ausland-Fernmeldeaufklärung zuständig ist. Wenn sich das Unabhängige Gremium an die G10-Kommission wenden wollte, mussten die Mitglieder erst einen Brief über das Kanzleramt schicken – also der Instanz, die eigentlich unabhängig kontrolliert werden soll. Ob sich dies geändert hat, ist unbekannt.

Der erste Bericht des Unabhängigen Gremiums an das Parlamentarische Kontrollgremium gibt weitere Hinweise auf mangelnde Kontrollbefugnisse und bestehende Kontrolllücken. Er beinhaltete de facto eine Aufzählung all dessen, was das UGr alles nicht hatte einsehen können. Problematisch war demnach häufig die Weigerung der Bundesregierung, dem UGr Zugriff auf Daten von ausländischen Nachrichtendiensten zu geben, mit einem Verweis auf die Third Party-Rule. Dieser Bericht ist öffentlich zwar nicht verfügbar, aber den Aussagen in der mündlichen Verhandlung nach konnte das UGr viele Suchbegriffe, die zwischen dem BND und ausländischen Nachrichtendiensten übermittelt wurden, nicht einsehen. Zudem, so die aussagende BGH-Richterin Cirener, habe das Unabhängigen Gremium in keinem einzigen Fall eine Absichtserklärung zu SIGINT-Kooperationen des BND mit ausländischen Partnerdiensten einsehen können. Auch habe man auch erst im März 2019 Zugang zur Dienstvorschrift “DV SIGINT” erhalten. Darüber hinaus ist nicht davon auszugehen, dass der BfDI alle im Rahmen des Verfahren bekannt gewordenen Dienstvorschriften des BND zur strategischen Fernmeldeaufklärung einsehen konnte, obwohl der BfDI schon heute die unabhängige Prüfung der Datenverarbeitung im Bereich der Ausland-Ausland-Fernmeldeaufklärung übernehmen soll.

Es ist zu hoffen, dass derartige Defizite nach dem nun gefällten Grundsatzurteil bald der Vergangenheit angehören. Die Verfassungshüter haben unmissverständlich festgelegt, dass die Anforderungen an die Rechtskontrolle der Auslandsaufklärung besonders hoch und detailliert zu sein haben (Rn. 273). Die Überwachung wird schließlich “anlasslos gegenüber jeder Person erlaubt und ist allein durch bestimmte Zwecksetzungen final angeleitet” (Rn 150). Ihre Kontrolle hat daher einen Ausgleich zu gewährleisten für den Ausfall “üblicher(r) rechtsstaatliche(r) Sicherungen” wie das Gebot des effektiven Rechtsschutz nach Art. 19 Abs. 4 Grundgesetz. Zudem hat sie die “gebotene verfahrensmäßige Strukturierung der Handhabung der (Überwachungs) befugnisse” (Rn. 273) abzusichern. Sprich: Neben der gerichtsähnlichen Vorabprüfung sämtlicher Überwachungsanträge der strategischen Fernmeldeaufklärung bedarf es der begleitenden Kontrolle der Datennutzung, -kenn-

zeichnung, -löschung, und -übermittlung. Diese zentralen Aufgaben können dem Urteil zufolge “nach den geltenden Regeln von vornherein durch das Unabhängige Gremium und die Kontrolle des Bundesdatenschutzbeauftragen von den Befugnissen und von der organisatorischen wie institutionellen Ausgestaltung her nicht in der verfassungsrechtlich gebotenen Weise sichergestellt werden” (Rn. 324).

Ein “Weiter so” kann es also nicht geben. Der Gesetzgeber muss die Kontrollarchitektur umfassend reformieren, wenn Deutschland weiterhin an diesem besonders sensiblen Instrument festhalten will. Als Richtschnur hat das Bundesverfassungsgericht insbesondere erhöhte und klarer definierten Schwellen für die Überwachung eingefordert sowie außerdem die Unabhängigkeit der neu zu schaffenden Rechtskontrolle angemahnt. “Die Kontrollinstanzen müssen in ihrer Arbeit von Einflussnahmen wirksam abgeschirmt und insoweit mit vollständiger Unabhängigkeit ausgestattet sein.” (Rn. 281).

Um das Ziel einer “Ende-zu-Ende” Kontrolle zu gewährleisten, also einer Aufsicht, die bereits vor der Datenerhebung das Genehmigungsverfahren mitverantwortet und danach sämtliche Analyse- und Datennutzungsverfahren begleitend prüft (Rn. 279), braucht es zwei eng verzahnte Instanzen der Rechtskontrolle. Weil keiner der aktuellen Spruchkörper dies garantieren kann, plädieren wir für die Schaffung eines Rats der deutschen Nachrichtendienst-Kontrolle – und eine Abschaffung der G10-Kommission und des Unabhängigen Gremiums bei gleichzeitiger Stärkung des BfDI als alleinige Instanz der administrativen Rechtskontrolle. Vorausgesetzt ist diesem Vorschlag, dass der Kontrollrat eine deutliche Stärkung des Mandats im Nachrichtendienstrecht erfährt und die neuen Arbeitsstrukturen mit zahlreichen hauptamtlichen Kontrolleur:innen besetzt werden.

II.2 Übersicht der zentralen Institutionen

In diesem Kapitel werden wir die wesentlichen Institutionen in ihrem veränderten, erweiterten oder neuen Tätigkeitsfeld gemäß unseres Vorschlages kurz vorstellen.

II.2.1 Rat der deutschen Nachrichtendienst-Kontrolle

Der neu geschaffene Rat der deutschen Nachrichtendienst-Kontrolle wird zum Dreh- und Angelpunkt des Grundrechtsschutzes und der Rechtskontrolle. Dieses neue Organ ist im Vergleich zu den vorigen Aufsichtsgremien – G10-Kommission und Unabhängiges Gremium – personell stark ausgebaut

und in seinen Rechten gestärkt. Er verantwortet das Genehmigungsverfahren, also die Vorabprüfung der Zulässigkeit und Erfordernis von Überwachungsanträgen von Bundesnachrichtendienst und Bundesregierung. Dies gilt auch für internationale Kooperationen und Datenübermittlungen ins Ausland.

Dieser Kontrollrat ist als ein gerichtsähnlicher Spruchkörper, also ein Quasi-Gericht, für die gesamte strategische Fernmeldeaufklärung eingerichtet. Diese "gerichtsähnliche" Kontrolle ist eine Kernforderung des Bundesverfassungsgerichts (Rn. 275). Das setzt einen deutlichen Ausbau der Kontrollbefugnisse voraus, die zum Teil aus dem BND-Gesetz, aus dem Artikel 10-Gesetz und den BND-Dienstvorschriften zusammengeführt werden können, zum Teil aber auch neu verfasst werden müssen.

Mitunter wird in Regierungskreisen argumentiert, dass für diesen "gerichtsähnlichen Spruchkörper" eine enge Anbindung an die Exekutive nötig sei, weil so bei den auch in Zukunft bedeutsamen Kooperationen zu ausländischen Nachrichtendiensten die nötige Vertraulichkeit besser gewährleistet sei. Dem widersprechen wir. Es mag sein, dass Kooperationspartner Vorbehalte gegen eine stärkere Einbeziehung der parlamentarischen Kontrolle in die Prüfung der Datennutzung äußern. Darum geht es aber hier nicht. Schon die G10-Kommission ist laut Bundesverfassungsgericht eine vom "Parlament bestellte oder gebildete unabhängige Institution *innerhalb des Funktionsbereichs der Exekutive*"[2]. In ihrer langjährigen Praxis sind von dort keine vertraulichen Informationen an die Öffentlichkeit gedrungen und ihre demokratische Legitimation und Unabhängigkeit wird unter anderem dadurch gewährleistet, dass ihre Mitglieder durch das Parlamentarische Kontrollgremium gem. §15 Abs. I Satz 4 Artikel 10-Gesetz bestellt werden.[3] Denselben Wahlprozess schlagen wir auch für den neuen Kontrollrat vor. Der Kontrollrat wird dadurch nicht Teil der parlamentarischen Kontrolle. Die Bundesregierung könnte in zukünftigen Verträgen und Absichtserklärungen in SIGINT-Kooperationen mit ausländischen Nachrichtendiensten den Verweis auf den "Funktionsbereich innerhalb der Exekutive" nutzen, um etwaige Bedenken ausländischer Partner hinsichtlich einer Aufhebung der Third Party-Regel für die Instanzen der Rechtskontrolle zu entkräften. Dem Urteil zufolge hat der Gesetzgeber nun Bedingungen zu schaffen, sodass zukünftig "die "Third-Party Rule" den Kontrollinstanzen nicht mehr entgegengehalten werden kann" (Rn. 292).

2 siehe Bundesverfassungsgericht, Urteil vom 15.12.1970, 2 BvR 629/68 ("Abhörurteil").

3 Im Vergleich dazu wurden die Mitglieder des Unabhängigen Gremiums laut § 15 Abs. 2 BND-Gesetz vom Bundeskabinett berufen.

Als weitere Neuerung ist in unserem Vorschlag vorgesehen, dass im Kontrollrat als "gerichtsähnlichen Spruchkörper" ein kontradiktorisches Verfahren eingeführt wird, wie es beispielsweise auch im U.S. FISA Court praktiziert wird. Das heißt, dass innerhalb des Kontrollrats unterschiedliche Interessen vertreten sind, zum Beispiel die von Bürgerrechtsanwält:innen. Das setzt voraus, dass neben den hauptamtlich beschäftigten Jurist:innen auch regelmäßig zwei weitere Personen den Sitzungen beiwohnen. Unserem Vorschlag nach sollte dies einerseits eine in grund- und menschenrechtsfragen umfassend geschulte Person sein, und andererseits eine Person, die das Vertrauen der Vertreter:innen von besonders schützenswerter Kommunikation (z.B. Anwält:innen, Journalist:innen, Gläubige) genießt. Zur Wahrung ihres besonderen Rechts auf Vertraulichkeit zur Erfüllung ihrer demokratischen Funktionen hat Karlsruhe die Bundesregierung mit dem Urteil erstmals ausdrücklich verpflichtet (Rn. 193).

Ziel ist es, dass diese beiden Personen gegenüber den Vertreter:innen der Ministerien, die die neuen Überwachungsmaßnahmen beantragen, eine unabhängige, kontradiktorische Position einnehmen und verteidigen können, damit das Verfahren nicht zu einseitig auf die Interessen der Sicherheitsbehörden ausgerichtet ist. Warum das so wichtig ist, hat unlängst ein Bundesrichter am FISA Court wie folgt beschrieben: „Um zu vermeiden, dass der Prozess zu einem Schau- und Stempelgericht wird, brauchte es einen Gegner, der bei allem, was dem FISA-Gericht vorgelegt wird, die Position der anderen Seite einnimmt. Richterinnen und Richter sind im Recht geschult, aber jeder, der einmal Richterin oder Richter war, wird Ihnen sagen, dass man beide Seiten eines Falles hören muss, ehe man entscheidet."[4]

II.2.2 Bundesdatenschutzbeauftragter

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wird unserem Vorschlag nach federführend bei der administrativen Rechtskontrolle. Karlsruhe hat es dem Gesetzgeber offengelassen, ob "die administrative Rechtskontrolle durch den Bundesdatenschutzbeauftragten oder durch eine verselbständigte Kontrollinstanz gewährleistet werden soll" (Rn. 281). Wir glauben, dass die administrative Rechtskontrolle ein so umfassendes Aufgabenpaket ist, dass sie von Fachleuten in einem Haus gebündelt werden sollte, aber eine ständige Rückkopplung zum Kontrollrat wichtig ist. Die administrative Rechtskontrolle hat "den gesamten Prozess der strategischen Überwachung auf seine Rechtmäßigkeit zu prüfen" (Rn. 276). Bereits

4 Eigene Übersetzung. Original: "to avoid being a rubber stamp, the process needed an adversary ... to challenge and take the other side of anything that is presented to the FISA Court. Judges are learned in the law and all that, but anybody who has been a judge will tell you that a judge needs to hear both sides of a case before deciding."

heute besitzt die G10-Kommission laut §15 Abs. 5 Satz 2 Artikel 10-Gesetz eine “Kontrollbefugnis”, die sich über das Genehmigungsverfahren “auf die gesamte Verarbeitung der nach diesem Gesetz erlangten personenbezogenen Daten der Nachrichtendienste des Bundes” erstreckt. Dieser Befugnis wird die G10-Kommission in ihrer jetzigen Ausstattung aber nicht in ausreichenden Weise gerecht. Bisher ist der BfDI von dieser Kontrolle ebenfalls weitestgehend ausgenommen, was sich grundlegend ändern muss. Die gesamte Fernmeldeaufklärung sollte ins Visier der hauptamtlichen und technisch versierten Kontrolleur:innen des BfDI geraten.

Außerdem treten die Mitarbeitenden des BfDI weiterhin auf den Plan, um beispielsweise Dateianordnungen zu prüfen und anlassbezogen Hinweisen auf Nichteinhaltung des Datenschutzes nachgehen zu können. Mit Blick auf die Anforderungen der internationale Kooperationspartner an die Ausgestaltung der Third Party-Regel könnte es nötig werden, zusätzliche Referate beim BfDI mit besonderen Geheimhaltungsvorschriften ausstatten zu müssen.

Wichtig ist, dass der Kontrollrat und der BfDI im engen Austausch miteinander stehen. Damit soll gewährleistet werden, dass Vorgaben des Kontrollrates vom BfDI den gesamten Verlauf der Datennutzung entlang geprüft werden können. Ein Beispiel: Ein Überwachungsantrag könnte vom Kontrollrat nur unter der Voraussetzung erteilt werden, dass bestimmte Daten nicht erhoben oder einzelne Netze gar nicht erst überwacht werden dürfen. Diese Genehmigung erteilt der gerichtsähnliche Spruchkörper, doch die tatsächlich Prüfung auf Einhaltung der Vorgaben seitens des BND muss durch die administrative Kontrolleinheit des BfDI erfolgen. Der “unabhängigen Rechtskontrolle administrativen Charakters” kommt damit keine abschließende Entscheidungsbefugnis zu (Rn. 276), es bedarf aber mindestens eines Beanstandungsrechts. Da unserem Vorschlag nach auch der Kontrollrat zumindest stichprobenartig den Grundrechtsschutz überprüfen können soll, sollten Kontrollrat und BfDI die Praxis gemeinsamer Kontrollbesuche fortsetzen und verstetigen, wie es bisher schon G10-Kommission und BfDI machen.[5]

II.2.3 Parlamentarische Kontrolle

2016 hat der Gesetzgeber die parlamentarische Kontrolle umfassend reformiert, insbesondere durch die Schaffung des Ständigen Bevollmächtigen, eines Leitenden Beamten sowie vier Referaten mit ca. 35 Personen inner-

5 siehe dazu: Bertold Huber, Kontrolle der Nachrichtendienste des Bundes - dargestellt am Beispiel der Tätigkeit der G 10-Kommission, Zeitschrift für das gesamte Sicherheitsrecht, 2017, Seite 12.

halb der Bundestagsverwaltung. Eine "Ausweitung der parlamentarischen Kontrolle", wie im gegenwärtigen Koalitionsvertrag der Bundesregierung für den Fall der Verfassungsschutzreform vorgesehen, lasse sich laut Gericht "aus den im vorliegenden Verfahren geltend gemachten Grundrechten nicht ableiten" (Rn. 300). Die Parlamentarische Kontrolle habe vielmehr "eine eigene, nicht speziell auf die Rechts- und Grundrechtskontrolle begrenzte Funktion und ist Ausdruck der allgemeinen parlamentarischen Verantwortung für die sachgerechte und politisch angemessene Aufgabenwahrnehmung der Exekutive" (Rn. 300).

Gleichwohl gibt es auch bei der parlamentarischen Kontrolle zentrale Verbesserungsvorschläge, um die Wirksamkeit der politischen und finanziellen Kontrolle des Bundestages über die Nachrichtendienste des Bundes zu erhöhen. Als Strukturreform schlagen wir in diesem Bereich vor, das Parlamentarische Kontrollgremium unter dem Dach des PKGr mit dem Vertrauensgremium zusammenzulegen.

Es ist insbesondere im Lichte der Arbeitsbelastung der Abgeordneten nicht mehr zeitgemäß, den Mitarbeiterstab der PKGr-Mitglieder den Zugang zu Sitzungen zu verwehren. Außerdem wird auch bei der parlamentarischen Kontrolle der strukturellen Vernetzung mit den anderen Aufsichtsgremien im Bund und auf Länderebene zu wenig Beachtung geschenkt. Hierdurch können sich teils erhebliche Kontrolllücken ergeben. Es war beispielsweise bereits eine fraktionsübergreifende Forderung aus dem Abschlussbericht des NSU-Untersuchungsausschusses von 2013, dass sich das PKGr "im Falle kooperativer Tätigkeiten der Dienste in Bund und Ländern mit den Kontrollgremien der beteiligten Bundesländer ins Benehmen setzen" solle.[6] Dies gilt es nun durch die Errichtung von Austauschplattformen und Jahrestreffen bis zum Ende des Jahres 2021 endlich zu verstetigen.

Die Kooperation von Regierung und Nachrichtendiensten mit den Kontrollorganen sowie ihre Einhaltung von Rechtsnormen und Kontrollvorgaben sollte außerdem bei der Finanzkontrolle einen größeren Stellenwert bekommen. Dafür ist der regelmäßige Austausch zwischen Mitgliedern des PKGr und der Leitungsebene der Rechtskontrolle entscheidend, also künftig zwischen PKGr und Kontrollrat. Es ist nicht nachvollziehbar, warum die Trennung zwischen politischer Kontrolle durch das PKGr und einer anders gelagerten Finanzkontrolle durch das Vertrauensgremium weiter Bestand haben sollte. Auch diese Fragmentierung wollen wir beenden, indem wir vorschlagen, das Vertrauensgremium aufzulösen und dessen Befugnisse auf das PKGr zu

6 siehe BT-Drs. 17/14600, S. 865, Punkte 41-43.

übertragen.[7] Damit könnte das PKGr auch das Budget der Nachrichtendienste ins Visier nehmen, sofern Rechtsverstöße im Rahmen der Kontrolltätigkeit festgestellt würden.

II.2.4 Beirat

Wir schlagen zudem vor, einen Beirat zu gründen, der Kontrollrat und BfDI, aber auf Anfrage gegebenenfalls auch dem PKGr oder dem Bundestag (etwa im Rahmen von Untersuchungsausschüssen) beratend zur Seite steht. Mit dem Beirat würde in Deutschland ähnlich wie in den Niederlanden, Großbritannien oder Neuseeland die Möglichkeit geschaffen, dass sich Kontrolleur:innen in technischen, rechtlichen, geopolitischen und gesellschaftlichen Fragen ihrer Tätigkeit jederzeit externe Expertise einholen können.

Im Zentrum der Beratungen sollten, wie auch beim Technology Advisory Panel (TAP) des englischen Kontrollgremiums IPCO, "die Auswirkungen des technologischen Wandels und die Verfügbarkeit und Entwicklung von Techniken zur Nutzung von Ermittlungsbefugnissen bei gleichzeitiger Minimierung der Eingriffe in die Privatsphäre stehen."[8] Da die Rechtskontrolle im Kontrollrat dafür sorgen muss die Grundrechte durch Überwachung so wenig wie möglich zu beeinträchtigen, kann der Beirat hier wichtige Impulse für Innovationen liefern. Mitglieder des Kontrollrats und BfDI sollen zu jedem wissenschaftlichen oder technologischen Aspekt der Überwachungsmethoden Rat suchen können, sei es in einem spezifischen Fall oder in einem allgemeineren Kontext.

Der Beirat hätte keine eigenen Kontrollbefugnisse und würde in internationalen Kooperationen als Third Party gelten, weil dessen Mitglieder (anders als beim TAP) keinen gesetzlichen Geheimhaltungspflichten unterliegen würden. Die vorläufig zwölf Mitglieder des Beirats sollten Personen sein, die in einem transparenten Auswahlverfahren aus Wissenschaft, Zivilgesellschaft und Privatwirtschaft rekrutiert und vom Bundestag durch Zwei-Drittel-Mehrheit gewählt werden. Die Mitgliedschaft im Beirat soll insgesamt nicht länger als zwei Legislaturperioden andauern. Der Bundestag sollte den Beirat qua Wahl und durch die Aufnahme ins Nachrichtendienstrecht legitimieren. Im Gesetz sollte auch festgelegt werden, dass der Beirat dem Bundestag einen Jahres-

7 Eventuell könnten die zukünftig durch die personelle Stärkung der G10-Kommission nicht mehr so stark ausgelasteten Stellen in der Bundestagsverwaltung, insb. das für die Vorbereitung der G10-Sitzungen zuständige Referat PK 4, für die Vorbereitung der Finanzkontrollen eingesetzt werden.

8 Zu den Aufgaben und Funktionsweisen des Technological Advisory Panel, siehe: TAP Working Protocol, 25 März 2019, abrufbar unter: https://www.ipco.org.uk/docs/TAP%20working%20protocol%20(25%20March%202019)%20FINAL.pdf

bericht über seine Aktivitäten vorzulegen hat. Der Bundestag hat den Beirat mit angemessenen Ressourcen, einschließlich Personal, auszustatten.

Die Mitglieder verfügen zusammen über eine ausgewogene wissenschaftliche und praktische Expertise im IT- und Sicherheitsrecht, dem Telekommunikationssektor, der Verwaltungswissenschaft, der internationalen Sicherheitspolitik sowie des Gefahrenabwehrrechts. Der Beirat sollte die Vielfalt innerhalb der Gesellschaft widerspiegeln, bei seiner Besetzung also beispielsweise auch Faktoren wie Geschlecht oder kultureller Hintergrund der Mitglieder berücksichtigen. Ebenfalls repräsentiert werden sollten besonders schützenswerte Berufsgruppen, deren Kommunikation von Überwachung besonders gefährdet und gleichzeitig aber besonders schützenswert ist, wie zum Beispiel Journalistinnen. Der Beirat sollte gemäß eines Verhaltenskodex für wissenschaftliche Beratungskomitees arbeiten. Insbesondere werden seine Mitglieder im öffentlichen Interesse handeln und höchste Standards für öffentliche Ämter einschließlich Unparteilichkeit, Integrität und Objektivität einhalten.

II.3 Konsequenzen

Die Folgen dieser Neustrukturierung sind weitreichend: Das Unabhängige Gremium und die G10-Kommission würden ebenso abgeschafft wie das Vertrauensgremium, außerdem müssten neben dem BND-Gesetz auch noch das Artikel 10-Gesetz sowie das PKGr-Gesetz umfassend reformiert werden. Es wäre jedoch aus unserer Sicht eine logische und notwendige Konsequenz aus dem ersten Grundsatzurteil zur BND-Fernmeldeaufklärung im digitalen Zeitalter. Der Reformdruck ist jetzt so hoch, weil die Bundesregierung jahrelang immer nur Minimaländerungen vorgenommen hat, anstatt die Kontrolle des massenhaften Datenabgreifens an die Digitalisierung anzupassen. Die Maxime war, rechtliche Graubereiche nach Skandalen zu legalisieren, anstatt sie verfassungsrechtlich auszubalancieren. Rechtssicherheit ging vor Rechtsstaatlichkeit. Wann aber, wenn nicht nach einem Grundsatzurteil aus Karlsruhe mitsamt der Bescheinigung einer bis dato verfassungswidrigen Praxis, könnte das politische Momentum für einen “großen Wurf” besser sein als jetzt?

Wenn die Bundesregierung jetzt unnötigerweise auf Tempo setzt und politisch nur unbedingt notwendige juristische Veränderungen als Konsequenz aus dem Karlsruher Urteil zulässt, dann läuft dies wohl auf das nächste “Reförmchen” am BND-Gesetz im Spätsommer oder Herbst hinaus. Hierbei könnten dann vermutlich in großen Teilen Textbausteine aus den bestehen-

den vier Dienstvorschriften – DV SIGINT, DV Übermittlung, DV Auftragsprofil und DV Internationale Absprachen mit ausländischen Nachrichtendiensten (Rn. 14) – ins BND-Gesetz übernommen werden. Damit würde die Bundesregierung dem Karlsruher Urteilsspruch in vielerlei Hinsicht aber nicht gerecht. Außerdem würde sie die Möglichkeit einer echten Harmonisierung des Nachrichtendienstrechts verstreichen lassen. Der Gesetzestext würde sich zwar ändern, aber nur ein Teil der Praxis – und damit würde dem Schutz der Grundrechte, an den das Grundgesetz die Bundesregierung im In- und Ausland bindet, nicht ausreichend Genüge getan. Was hingegen für die Kontrollpraxis konkret gewonnen wäre, wenn man die Schutznormen und das Kontrollgefüge grundlegend umstrukturiert und zusammenlegt, zeigen wir im folgenden Teil.

III. Folgen für die Überwachungspraxis

Der erste Kontrollschritt zum Grundrechtsschutz beginnt, bevor der BND überhaupt erst Daten erhebt – nämlich in der Begrenzung seiner Befugnisse und strengen Auflagen für die Datenverarbeitung und -übermittlung. "Eine globale und pauschale Überwachung lässt das Grundgesetz auch zu Zwecken der Auslandsaufklärung nicht zu", heißt es im Urteil (Rn. 168). Der Gesetzgeber müsse die Befugnisse daher auf konkrete und begrenzte Zwecke beschränken.

Dies sei im aktuellen BND-Gesetz nicht der Fall: § 6 BNDG ermächtigt den BND beispielsweise Daten schon für die "Handlungsfähigkeit Deutschlands" oder "sonstige Erkenntnisse von außen- und sicherheitspolitischer Bedeutung" zu erheben. Diese "weit und offen formulierten Zwecke", schreibt das Gericht, "verfehlen diese Anforderungen deutlich" (Rn. 305).

Die zentralen Anforderungen für die Überwachung – und damit unweigerlich auch für den gesamten Kontrollprozess – sind laut Urteil:

- Die Überwachung nach dem Artikel 10-Gesetz (Inland-Ausland) und dem BND-Gesetz (Ausland-Ausland) sind "gleichermaßen an Art. 10 Abs. 1 GG zu messen" (Rn. 172).
- Die Überwachung zur Gefahrenfrüherkennung muss eingeschränkt werden auf "begrenzte und differenzierte Zwecke", zum Beispiel zum "Schutz hochrangiger Gemeinschaftsgüter" wie der Sicherung des Friedens (Rn. 176).
- Überwachungsmaßnahmen abseits der Gefahrenfrüherkennung, die "allein das Ziel der Information der Bundesregierung und der Vorbereitung von Regierungsentscheidungen haben", können dann erlaubt werden, wenn eine Zweckänderung und eine Weiterleitung ins Ausland ausgeschlossen sind (Rn. 177).
- Eine anlasslose Inlandsüberwachung von Deutschen oder in Deutschland befindlichen ausländischen Personen mit Mitteln der strategischen Fernmeldeaufklärung kommt "von vornherein nicht in Betracht" (Rn. 171).[9]
- Berufsgruppen, die besonders auf die Vertraulichkeit ihrer Kommunikation angewiesen sind, müssen vor strategischer Überwachung besonders

9 Das Gericht hat die Frage offen gelassen, ob die Abstufung im aktuellen BND-Gesetz zwischen Deutschen und EU-Bürger:innen verfassungskonform ist, weil dies nicht Gegenstand des Verfahrens war. Die Reform sollte im Sinne des 1. Leitsatzes, der Art. 10 GG als Abwehrrecht alle Menschen weltweit schützt, den Schutz von EU-Bürger:innen entsprechend stärken.

geschützt werden (Rn. 195). Hierzu zählen zum Beispiel Journalist:innen sowie Anwält:innen.

- Der Kernbereich privater Lebensgestaltung, umgangssprachlich auch als Intimsphäre bezeichnet, darf unter keinen Umständen im Rahmen staatlicher Überwachung erfasst oder verwertet werden. Dies folgt aus der Menschenwürdegarantie des Grundgesetzes und gilt für alle Menschen, unabhängig ihrer Nationalität (Rn. 199).

In der Reform müsste dafür an diversen Stellschrauben gedreht werden, um den verfassungsrechtlichen Anforderungen an die strategische Überwachung zu genügen. Hierzu zählen insbesondere eine Begrenzung der Zwecke zur Überwachung im Artikel 10-Gesetz sowie BND-Gesetz (III.1), die Verbesserung von Filtertechniken (III.2) inklusive der Einführung von Schutzlisten (III.3) und innovativer Datenverarbeitungstools zur Einhaltung der Zweckbindung (III.4). Neue Anforderung für die Kontrollpraxis ergeben sich ebenfalls für Übermittlungen von Daten (III.5), wobei zwischen inländischen (III.5.2) und Übermittlungen ins Ausland (III.5.3) nochmals unterschieden werden muss.

Bei einer Novellierung des Nachrichtendienstrechts ist zudem darauf zu achten, dass die zahlreichen mehrgliedrigen Verweisungsketten im Sinne der Normenklarheit zu vermeiden, besser noch: aufzuräumen sind. Verweisungen dürfen "nicht durch die Inbezugnahme von Normen, die andersartige Spannungslagen bewältigen, ihre Klarheit verlieren und in der Praxis nicht zu übermäßigen Schwierigkeiten bei der Anwendung führen. Unübersichtliche Verweisungskaskaden sind mit den grundrechtlichen Anforderungen daher nicht vereinbar." (Rn. 215). Als ein Beispiel wird "§ 24 Abs. 3 BNDG in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG" genannt, "der zu einer Übermittlung von Informationen im Kontext von Staatsschutzdelikten an Polizeien und Staatsanwaltschaften ermächtigt." (Rn. 312)

III.1 Strengere Eingriffsbefugnisse im BND-Gesetz

Bisher regelt das Artikel 10-Gesetz die sogenannte "internationale Kommunikationsüberwachung", die einen Inlandsbezug hat, während das BND-Gesetz auf die Ausland-Ausland-Überwachung zielt, in der sich also ausländische Personen im Ausland befinden. Dieser Trennung lag die falsche Annahme der Bundesregierung zugrunde, dass Artikel 10 Grundgesetz im Ausland nicht gelte. Da Karlsruhe nun festgestellt hat, dass die Überwachung "gleichermaßen an Art. 10 GG zu messen" sei, ergibt eine solche Zweckbindung an die Nationalität keinen Sinn mehr. Stattdessen empfehlen wir, die Überwachung

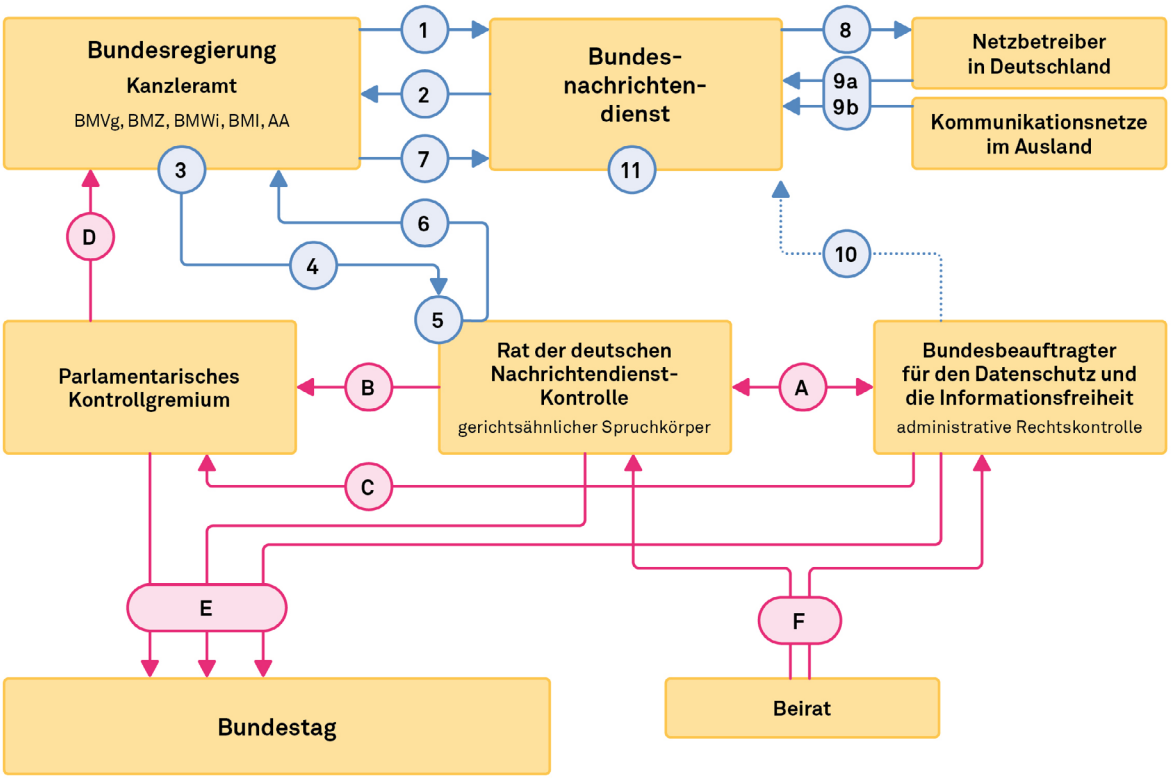
nur noch durch inhaltliche Kriterien zu legitimieren, wobei hier im Sinne des Karlsruher Urteils zwischen Gefahrenfrüherkennung und der allgemeinen, nachrichtendienstlichen Aufklärung zu unterscheiden wäre (Rn. 175-177).

Für die Gefahrenfrüherkennung listet § 5 Artikel 10-Gesetz bereits heute die Voraussetzungen auf, unter denen eine strategische Überwachung mit Grundrechtsbezug möglich ist. Diesen Katalog gilt es bei der Reform als Referenz für die gesamte strategische Überwachung des Bundesnachrichtendienstes zu verwenden. Die mündliche Verhandlung in Karlsruhe hat gezeigt, dass diese Liste offensichtlich geeignet ist, die Erfassung auf das zwingend Notwendige zu beschränken: Während nach Art.10-Gesetz etwa 230 Kommunikationsinhalte in einem halben Jahr erfasst würden, seien es nach BND-Gesetz 154.000 Inhalte pro Tag, also circa 28 Millionen in einem halben Jahr. Der Bezug auf die Zwecke im Artikel 10-Gesetz für die gesamte strategische Überwachung hat außerdem den Vorteil, dass beim Bundesverfassungsgericht hierzu eine weitere Verfassungsbeschwerde anhängig ist, mit dessen Entscheidung in absehbarer Zeit zu rechnen sein dürfte. Damit erhielten alle Seiten – nicht zuletzt der BND selbst – Klarheit, ob die Voraussetzungen aus dem Artikel 10-Gesetz den verfassungsrechtlichen Anforderungen genügen. Im Ergebnis wäre es im Sinne der Normenklarheit sinnvoll, den Teil der strategischen Fernmeldeaufklärung komplett aus dem Artikel 10-Gesetz herauszulösen und in Gänze im BND-Gesetz zu verankern – der Bundesnachrichtendienst ist ohnehin die einzige Behörde, die dieses Instrument nutzen darf.

Geringere rechtliche Hürden sollen in Zukunft gelten, wenn die Ausland-Ausland-Fernmeldeaufklärung allein dazu dient, die Bundesregierung in ihrem Regierungshandeln zu informieren und ihre außen- und sicherheitspolitische Handlungsfähigkeit zu garantieren. Dies kann jedoch kein “Freifahrtschein” für die schrankenlose Überwachung werden, denn “eine solche gesetzliche Begrenzung (kann) nicht durch das allein politisch definierte Auftragsprofil der Bundesregierung ersetzt werden” (Rn. 305). Insofern ist auch für diese Überwachung zu fordern, dass konkrete Eingriffsschwellen im Gesetz benannt werden. Diese können möglicherweise weiter sein als bei der Gefahrenfrüherkennung, aber sie müssen so konkret sein, dass bei einer Antragsprüfung (ex ante) und späterer Prüfung der Datenverarbeitung (ex post) die Kontrolleffektivität durch Kontrollrat, BfDI und PKGr gewährleistet ist.

Kontrollablauf bei Datenerhebung zur strategischen Fernmeldeaufklärung

Stiftung Neue Verantwortung



Verfahren pro Antrag

1. Aufklärungsinteresse der Bundesregierung
2. Antrag zur Überwachung bestimmter Netze
3. Prüfung des Antrags durch Fachaufsicht
4. Antrag zur Überwachung bestimmter Netze
5. Prüfung des Antrags durch Spruchkörper auf Rechtmäßigkeit und Notwendigkeit
6. Genehmigung (unter Auflagen) oder Ablehnung von Antrag
7. Beauftragung zur Datenerhebung
8. Verpflichtung privater Netzbetreiber zur Datenausleitung
9. **a)** Datenausleitung an BND
   b) Datenerhebung durch BND
10. stichprobenartige Kontrolle der Datenausleitung anhand datenschutzrechtlicher Kriterien durch BfDI
11. Datenverarbeitung beim BND

Kontrollvorgaben

- **A** regelmäßiger Austausch zu Anträgen (4) und Kontrollergebnissen bei Datenerhebungen (10)
- **B** regelmäßiger Bericht über Genehmigungen und Prüfergebnisse
- **C** regelmäßiger Bericht über Prüfergebnisse
- **D** anlassbezogene politische und finanzielle Kontrolle
- **E** Bericht an den Bundestag über Datenerhebung und Prüfergebnisse
- **F** ständige Beratung, z.B. zu technischer Entwicklung oder Menschenrechtssituation in bestimmten Ländern

Während bei der Gefahrenfrüherkennung in Eilfällen eine Ausnahme zur ex ante-Kontrolle durch den Spruchkörper erlaubt werden könnte, sollte strategische Überwachung zur allgemeinen Aufklärung generell unter einen ex ante-Vorbehalt gestellt werden. Dies ergibt sich daraus, dass es hier typischerweise an der Dringlichkeit fehlen dürfte (ist sie gegeben, greift die Regelung zur Gefahrenfrüherkennung). Ferner wird damit ein Missbrauch durch die tendenziell weiter gefassten Zwecke zur allgemeinen Aufklärung verhindert.

In beide Erfassungsgrundlagen – Gefahrenfrüherkennung und allgemeine Aufklärung – muss jeweils die besondere Schutzwürdigkeit bestimmter Kommunikationsbeziehungen festgeschrieben werden. Neben dem Verbot der reinen Inlandsüberwachung sowie des Kernbereichs privater Lebensgestaltung, zählt hierzu künftig auch erstmals die Kommunikation bestimmter Berufsgruppen. Hier stellte das Gericht klar, dass zum Beispiel allein die Aussicht auf nachrichtendienstlich relevante Informationen keine Rechtfertigung für die strategische Überwachung der Presse darstellt.[10] Regelungen aus der Strafprozessordnung (§§ 53, 160a) können hierfür als Orientierung dienen, dürfen jedoch nicht 1:1 übernommen werden. Gerade eine Einzelfallabwägung im Sinne des § 160a StPO gekoppelt an bestimmte Straftaten gibt es bei der strategischen Überwachung gerade nicht. Eine Lösung könnte sein, die Genehmigungen für die Überwachung der Berufsgruppen zeitlich stärker zu begrenzen, an höhere Voraussetzungen zu knüpfen und eine zweite Einzelfallprüfung nach der Erfassung einzufordern (Rn. 195), in der zumindest stichprobenartig durch die administrative Rechtskontrolle des BfDI kontrolliert wird, ob die Verhältnismäßigkeit gewahrt bleibt. Gibt es hieran Zweifel, müssen die Erkenntnisse an den Spruchkörper weitergeleitet werden, was eine Neubewertung der Genehmigung zur Folge hat.

III.1.1 Maschine-Maschine-Kommunikation

Dringender Regelungsbedarf besteht hinsichtlich der sogenannten Maschine-Maschine-Kommunikation. Laut Ausführungen der Bundesregierung im Verfahren erfasst der BND neben Verkehrs- und Inhaltsdaten aus

10 Gerade der Schutz von Journalist:innen ist eine Herausforderung, weil “Journalismus” kein geschützter Begriff ist und der Beruf durch seine grund- und menschenrechtliche Verankerung keine staatliche Zulassungsverfahren kennen kann. Im internationalen Kontext ist es erst recht herausfordernd, zwische Presse und Nicht-Presse zu differenzieren. Ein Ansatz könnte sein, dem BND nicht abzuverlangen, von vornherein jede Entscheidung mit absoluter Sicherheit treffen zu müssen, sondern gesetzliche Sorgfaltspflichten über die Informierung zur Lage der Pressefreiheit in den Ländern vorzusehen, in denen der BND überwacht. Siehe ausführlich: Moßbrucker, Daniel. 2020. Urteil zum BND-Gesetz. Quellenschutz im Zeitalter digitaler Massenüberwachung. Netzpolitik.org 25.05.2020, abrufbar unter: https://netzpolitik.org/2020/was-heisst-quellenschutz-im-zeitalter-digitaler-massenueberwachung/

Telekommunikation auch “andere in den Netzen transportierte Daten aus Mensch-zu-Maschine- oder Maschine-zu-Maschine-Kommunikation, wie beispielsweise automatisch abgesetzte Lokalisationsdaten eingeschalteter Mobiltelefone” (Rn. 10). In der mündlichen Verhandlung bestätigten Mitarbeiter des BND, dass für diese Maschine-Maschine-Kommunikation derzeit kein Grundrechtsschutz gemäß Artikel 10 gälte. Das Argument: Grundrechte können nur von Menschen wahrgenommen werden, nicht aber von Maschinen.

Zwar wollen wir nicht bestreiten, dass Grundrechte zuvorderst Abwehrrechte von Bürger:innen gegen die Staatsgewalt sind. Allerdings eröffnet eine rein technische Auslegung des Rechts hier große Schutzlücken. Erinnerungen an die “Weltraumtheorie” werden wach, in der ein Grundrechtsschutz vom BND verneint wurde, wenn Satellitenkommunikation im Weltraum außerhalb des Geltungsbereich des Grundgesetzes auf der Erde überwacht würde. In einer digitalen Gesellschaft, in der Menschen allumfassend von Technik umgeben sind, ist Maschine-Maschine-Kommunikation vielfach die notwendige Bedingung, um überhaupt Mensch-Mensch-Kommunikation zu ermöglichen. Gleichwohl kann diese Maschine-Maschine-Kommunikation selbstverständlich einen G10-Bezug haben: Die technischen Lokalisationsdaten eines Mobiltelefons, welches sich in die Funkzelle einwählt, lässt direkte Rückschlüsse auf das Bewegungsprofil eines Menschen zu. Mit dem Ausbau von 5G-Netzen und dem Internet der Dinge wird diese Bedeutung noch steigen: Das smarte Thermometer, welches im Winter jeden Abend um 19 Uhr die Heizung hochdreht, lässt beispielsweise darauf schließen, dass um diese Uhrzeit die Bewohner:innen nach Hause kommen.

In der Neuregelung des Nachrichtendienstrechts sollte daher klargestellt werden, dass auch Maschine-Maschine-Kommunikation einen Grundrechtsbezug haben kann und somit einem Schutzniveau wie rein menschliche Kommunikation unterliegt. Auch hier hilft statt einer technischen eine funktionale Betrachtungsweise: Entscheidend ist, was der Bundesnachrichtendienst mit den Daten machen will. Wenn sie rein technisch für die Optimierung von Filtertechniken genutzt werden, kann ein Grundrechtsbezug eher verneint werden als wenn Maschine-Maschine-Kommunikation zur Aufgabenerfüllung des BND – allgemeine Auslandsaufklärung für die Regierung und Gefahrenfrüherkennung – dient.

III.1.2 Binnenrecht vs. Gesetz

Mit dem Grundsatzurteil hat das Bundesverfassungsgericht auch festgestellt, dass vieles, was bisher in der Öffentlichkeit unbekannten Dienstvorschriften stand, in ein demokratisch legitimiertes Gesetzgebungsverfahren

eingebunden werden muss. Es kann nicht im "Binnenrecht" verbleiben, sondern gehört ins Gesetz selbst. Zwar brauchen "die einzelnen Schritten der Auswertung der erfassten Daten", so das Gericht, "nur mit Bezug auf die wesentlichen Grundlagen" im Gesetz verankert zu werden (Rn. 192), aber selbst das erfordert einige Novellierungen im Nachrichtendienstrecht.

Außerdem muss auch das verbleibende Binnenrecht einer "unabhängigen objektivrechtlichen Kontrolle" unterliegen (Rn. 192). Bis heute ist das nicht so. Laut unseren Gesprächen und Mitschriften aus der mündlichen Verhandlung hatten sowohl das Unabhängige Gremium als auch der BfDI, und wohl auch die G10-Kommission, keinen Zugriff auf die vier genannten Dienstvorschriften (DV SIGINT, DV Übermittlung, DV APB, DV Internationale Absprachen, Rn. 14).

III.2 Filterung geschützter Kommunikation

Angesichts der enorm gestiegenen Erfassungskapazitäten der strategischen Überwachung ist es nicht möglich, eigentlich geschützte Kommunikation ausnahmslos von der Erfassung auszunehmen. Wie Tagesschau[11] und Spiegel[12] vor der Urteilsverkündung berichteten, kann der BND derzeit jeden Tag auf 1,2 Billionen Internet-Verbindungen zugreifen. Bei einer Filterung nach IP-Adressen, die laut Bundesregierung mit 96 bis 98 prozentiger Wahrscheinlichkeit geschützte Kommunikation ausfiltere, blieben täglich jedoch immer noch rund 24 Milliarden Rohdaten übrig, die eigentlich schon vor der Verarbeitung gelöscht werden müssten. Solchen Filterprozessen kommt in Zukunft aufgrund der rasant steigenden Volumina internetbasierter Kommunikation eine zunehmende Bedeutung zu, und der BND muss in der Reform gesetzlich verpflichtet werden, diese Filter nach dem neuesten Stand der Technik laufend zu aktualisieren (Rn. 173).

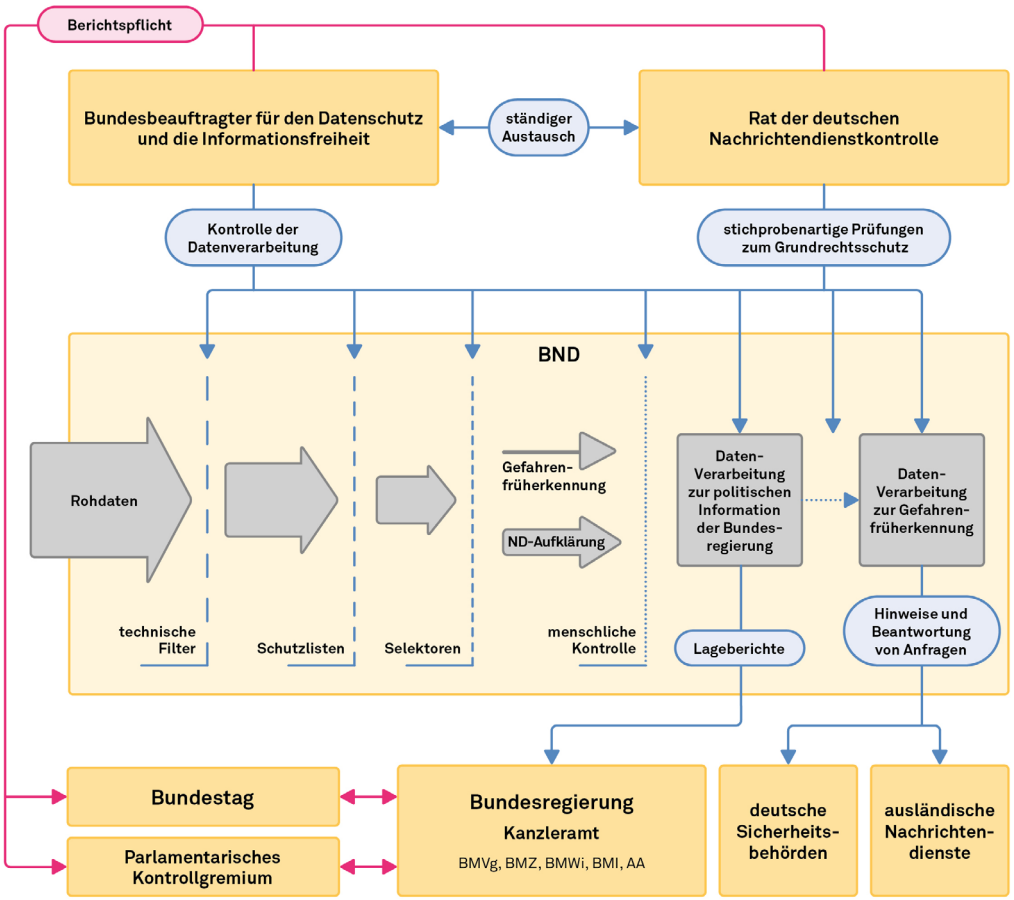
Ein erster Schritt zur Einbindung der Geheimdienstkontrolle in die Filterung sollte künftig darin liegen, dass der Spruchkörper bei der Genehmigung von Anträgen realistische – und damit grundrechtlich gebotene – Zielvorgaben macht, wie gut die Filter geschützte Kommunikation aussondern müssen. Diese Zielvorgaben müssen vom Bundesdatenschutzbeauftragten überprüft

11 Meyer-Fünffinger, Arne/Tanriverdi, Hakan & Zierer, Maximilian. 2020: So überwacht der BND das Internet. Auslandsgeheimdienst. Tagesschau.de 15. Mai 2020, abrufbar unter: https://www.tagesschau.de/investigativ/br-recherche/bnd-urteil-101.html

12 Hipp, Dietmar/Hoppenstedt, Max, Knobbe, Martin & Wiedemann-Schmidt, Wolf. 2020. BND kann bis zu 1,2 Billionen Verbindungen pro Tag abzweigen. Spiegel 15. Mai 2020, abrufbar unter: https://www.spiegel.de/netzwelt/netzpolitik/bnd-kann-bis-zu-1-2-billionen-verbindungen-pro-tag-abzweigen

und laufend an den Spruchkörper gemeldet werden. Stellt sich beispielsweise heraus, dass in einem Kommunikationsnetz der Anteil deutscher Inlandskommunikation so hoch ist, dass trotz Filterung ein nicht hinnehmbarer Anteil einer weiteren Verarbeitung unterläge, würde die Überwachung unverzüglich beendet werden müssen – mindestens solange, bis die Filter optimiert wären oder die Überwachung eingeschränkt würde. Es bräuchte dann einen neuen, vom Spruchkörper zu genehmigenden Antrag zur Überwachung.

Kontrollablauf bei der Datenverarbeitung im Rahmen der strategischen Fernmeldeaufklärung



III.3 Schutzlisten

Die für die Filterung wichtigste – und für die Kontrolle wohl auch heikelste – Neuerung betrifft die Einführung von Schutzlisten (sogenannte Positivlisten, häufig auch “Whitelists”). Laut Karlsruher Urteil ist es künftig verfassungsrechtlich geboten, den BND gesetzlich zur Pflege von Datenbanken zu verpflichten, um “Hinweise auf eine besondere Schutzwürdigkeit (...) bestimmter Personen zu sammeln und auf sie bezogene Telekommunikations-

kennungen in einer Weise zusammenzuführen, die die Filterung der Suchbegriffe und der für die Übermittlung vorgesehenen Daten ermöglicht" (Rn. 258). Im Klartext: Beim BND sollen Millionen Daten zu Kommunikation vorrätig gehalten werden, die potentiell hochinteressant wäre, faktisch aber nicht oder nur unter hohen Hürden überwacht werden darf.

Wie in der Verhandlung bekannt wurde, führt der BND bereits eine sogenannte "G10-Positivliste". Hier führt der Geheimdienst technische Merkmale, die erwiesenermaßen Deutschen oder sich in Deutschland aufhaltenden Personen zuzurechnen sind – und damit nicht überwacht werden dürfen im Rahmen der strategischen Überwachung. Diese G10-Positivliste fungiert dann als eine Art Qualitätsfilter, weil sie aus dem Rohdatenstrom "G10-Kommunikation" heraussiebt. Während etwa der DAFIS-Filter eher technischen Kriterien folgt und Telefonnummern mit +49-Kennung oder Websites mit der Top-Level-Domain .de aussortiert, handelt es sich bei dieser "G10-Positivliste" eher um ein qualitatives, und dennoch hochautomatisiertes, Filterverfahren.

Gemäß dem Urteil muss die BND-Reform die gesetzliche Grundlage für drei verschiedene dieser Schutzlisten berücksichtigen: Neben einer G10-Positivliste auch eine für den Kernbereichsschutz, worunter zum Beispiel Drogen- oder Schwangerschaftsberatungen, Telefonseelsorge, Sex-Hotlines oder digitale Anlaufstellen der Gesundheitsämter oder Arztpraxen fallen könnten. In solchen Fällen ist zu erwarten, dass ausschließlich die Intimsphäre betreffende Kommunikation überwacht würde, was im Hinblick auf die Menschenwürdegarantie des Grundgesetzes verboten wäre.

Auch für den Schutz von Berufsgruppen mit besonders sensiblen Kommunikationsbeziehungen sollen solche Schutzlisten eingeführt werden müssen (Rn. 258). Der BND könnte also alle Telekommunikationsmerkmale sammeln, die erwiesenermaßen von Journalist:innen oder Anwält:innen genutzt würden. Anders als beim G10- und Kernbereichsschutz ist eine Überwachung in diesen Fällen jedoch nicht grundsätzlich ausgeschlossen, sondern unterliegt einer höheren Prüfung – und damit erhalten diese Listen eine gänzlich andere Brisanz.

Der theoretische Nutzen ist klar: Um nicht systematisch, und wenn auch nur "aus Versehen", zum Beispiel Redaktionen abzuhören, gibt es ein Verzeichnis mit ihren Telefon- und Internetanschlüssen. Dieses kann eine "Warnung" für den BND sein. Gerade bei internationalen Kooperationen mit ausländischen Nachrichtendiensten kann eine solche Liste als "rote Linie" dienen: Was sich auf der Liste befindet, darf der BND nicht an autokratische Regime

weiterreichen, die damit vielleicht physisch gegen kritische Journalist:innen oder Menschenrechtsanwält:innen vorgehen würden. “Der Staat darf seine Hand nicht zu Verletzungen der Menschenwürde reichen.” (Rn.237). Der BND würde damit technisch sicherstellen können, dass im Rahmen von automatisierten Kooperationen ausländische Dienste diese Personen nicht mittels BND-Infrastruktur überwachen können.

Es sollte daher im Gesetzgebungsverfahren erörtert werden, ob es einen Rechtsanspruch zur Aufnahme auf solche Schutzlisten geben könnte. Dieser sollte dann nicht nur für Deutsche gelten, sondern auch für ausländische Personen, die sich mit ihren Telekommunikationsmerkmalen eintragen könnten, sei es G10, Kernbereich oder Berufsgeheimnisträger:innen. Ob die Personen Anspruch darauf haben, würde vom Spruchkörper entschieden und den Personen mitgeteilt. Der Rechtsweg gegen eine Entscheidung müsste ihnen offen stehen. Es braucht außerdem ein Verfahren, das regelmäßig sicherstellt, dass die Personen die gemeldeten Telekommunikationsmerkmale noch nutzen, zum Beispiel über Opt-ins. Hier könnte der neu zu schaffende Beirat einen ersten Beratungsauftrag erhalten.[13]

Praktisch birgt jedoch gerade die Liste zu Berufsgeheimnisträger:innen enormes Missbrauchspotential. Bei einigen – insbesondere Anwält:innen sowie Journalist:innen – ist eine Überwachung zwar an hohe Hürden geknüpft, aber möglich. Gerade ihre Kommunikation dürfte für den BND aufgrund der Nähe zu seiner Tätigkeit (Informationsrecherche, Einblick in Strafverfahren etc.) auch besonders “interessant” sein. Dies rechtfertigt eine überdurchschnittlich hohe Kontrolldichte seitens des Spruchkörpers und Bundesdatenschutzbeauftragten. Die Listen müssen letztlich auch den Kontrollorganen als Referenz dienen zur Beurteilung, ob die “Abwägung” ausgewogen ist oder systematisch zugunsten Überwachung des BND führt.[14]

13 Orientierung könnte hier das Berliner Funkzellen-Transparenz-System (FTS) bieten. Auch hier können Menschen sich mit ihrer Handynummer registrieren, um zu erfahren, ob sie bei einer nicht-gezielten, massenhaften Datenauswertungen erfasst wurden, siehe: https://fts.berlin.de/

14 Eine weitere, technische Möglichkeit zur Wahrung der Vertraulichkeit dieser eigentlich schützenswerten Kommunikation könnte darin bestehen, personenbezogene Daten bei der menschlichen Verarbeitung systematisch in Hashwerte umzuwandeln. Dies sind verschlüsselte Codes, die auf genau einen Ursprungswert hinweisen (z.B. eine Telefonnummer). Der sogenannte MD5-Hash zu 030 1000 2000 ist beispielsweise 3cb7b85fc4f111a0a13f4819d88329bd. Bei diesem Hash ist sichergestellt, dass keine andere Telefonnummer diesen Hashwert haben kann. Allein aus dem Hashwert lässt sich jedoch auch kein Rückschluss auf die Telefonnummer ablesen. Für die BND-Auswertung hätte dies den Vorteil, dass zum Beispiel Kommunikationsnetzwerke durch Metadaten-Analysen Kommunikation mit “journalistischer Beteiligung” weiterhin möglich wären, aber hierbei keine Klarkennungen von Journalist:innen sichtbar genutzt werden müssten.

III.4 Innovative Verfahren der Zweckbindung

Im Laufe der Arbeit mit Informationen aus der strategischen Überwachung innerhalb des Bundesnachrichtendienstes muss sichergestellt werden, dass die Informationen nur zu den Zwecken verarbeitet werden, die vorab vom Kontrollrat genehmigt wurden. Dies scheint besonders wichtig im Hinblick auf die Unterscheidung von "Gefahrenfrüherkennung" und "allgemeine nachrichtendienstliche Aufklärung zur politischen Information der Bundesregierung". Für letztere hat das Bundesverfassungsgericht nur dann geringere Hürden bei der Überwachung erlaubt, wenn sichergestellt ist, "dass eine Zweckänderung insoweit prinzipiell ausgeschlossen ist und die (...) gewonnen Erkenntnisse (...) nicht an andere Stellen weitergeleitet werden dürfen" (Rn. 177).

Wir schlagen daher vor, künftig zwei komplett getrennt voneinander organisierte Auswertungseinheiten mit getrennten IT-Systemen innerhalb des BND aufzubauen (siehe zu datengeschützten Möglichkeiten der Zweckwahrung auch Kapitel IV. 2.3). Die Einheit zur Gefahrenfrüherkennung erhält nur Überwachungsdaten, die mit Selektoren ausgefiltert wurden, die den strengeren Anforderungen des aktuellen § 5 Artikel 10-Gesetz genügen. Diese Überwachungsdaten haben auch bei der Auswertung höhere Auswertungsschwellen, zum Beispiel bezüglich des Schutzes bestimmter Berufsgruppen wie Journalist:innen (Rn. 193). Diese höheren Hürden sind nötig, weil die Gefahrenfrüherkennung eine Übermittlung an Einheiten der Strafverfolgung deutlich wahrscheinlicher macht, womit die potentiellen Folgen und Grundrechtseingriffe für die Betroffenen schwerer wiegen (Rn. 185, 186).

Davon – auch räumlich – getrennt sollte eine Auswertungseinheit angesiedelt werden, die nur Daten erhält, die mittels Selektoren zur "allgemeinen nachrichtendienstlichen Aufklärung" ausgesiebt wurden. Diese Überwachungsdaten sollten bei den Analyst:innen nur so verfügbar gemacht werden, dass personenbezogene Daten wie zum Beispiel Metadaten (Telefonnummern, Email-Adressen) unkenntlich bleiben. Auf sie wird es für Regierungsberichte "oft schon nicht ankommen, sodass diese ausgesondert werden können und gegebenenfalls müssen" (Rn. 225). Eine technische Lösung könnte sein, dass technische Metadaten automatisch verschlüsselt werden, ehe sie in die Auswertung kommen. Auch Inhalte, zum Beispiel der Text einer E-Mail, könnte zuvor mittels Künstlicher Intelligenz auf personenbezogene Daten hin untersucht werden, wie beispielsweise "Sincerely, Tom Hanks". Benötigen die Auswertungseinheiten solche personenbezogenen Daten, etwa um die Glaubwürdigkeit einer Quelle einschätzen zu können, können

sie BND-intern eine Entschlüsselung beantragen – dies muss jedoch protokolliert und der Kontrolle zugänglich sein. Damit würde erkennbar, wie oft von dieser "Ausnahme" Gebrauch gemacht würde.

Daten können zwischen der Auswertung zur Gefahrenfrüherkennung und der nachrichtendienstlichen Aufklärung nur ausgetauscht werden, wenn diese Zweckänderung ex ante vom Kontrollrat genehmigt wurde. In Eilfällen, zum Beispiel bei Gefahr für Leib und Leben in Entführungsfällen, kann diese Genehmigung ex post eingeholt werden.

III.5 Vorgaben für Übermittlungen und internationale Kooperationen

Da der Bundesnachrichtendienst Daten naturgemäß nicht als Selbstzweck erhebt, sondern gerade als Behörde ohne operative Befugnisse im Kern seiner Arbeit vor allem an inländische und ausländische Stellen weiterleitet, kommt den Regelungen zur Datenübermittlung in der künftigen Überwachungs- und Kontrollpraxis eine hohe Bedeutung zu. Im Folgenden werden wir zunächst beleuchten, welche allgemeinen Anforderungen an Übermittlungen Karlsruhe im Urteil aufstellt (III.5.1), ehe wir die Folgen für die Praxis bei inländischen Übermittlungen (III.5.2), bei Übermittlungen ins Ausland (III.5.3.1) sowie bei internationalen, automatisierten Kooperationen (III.5.3.2) im Lichte des von uns vorgeschlagenen Kontrollgefüges diskutieren.

III.5.1 Grundsätze für Datenübermittlungen

Nach der Erhebung begründet die Übermittlung personenbezogener Daten durch den BND an andere Stellen einen neuen Grundrechtseingriff (Rn. 212). Grundsätzlich sollen Daten nur für solche Zwecke übermittelt werden, für die die Überwachung genehmigt worden war. Mit dieser Zweckbindung soll ein Missbrauch der Datennutzung verhindert werden. Grundsätze für die Datenübermittlung durch den BND sind:

- Es braucht eine eigene Rechtsgrundlage für die Datenübermittlung (Rn. 214) und die Zwecke der Übermittlungen müssen den Verhältnismäßigkeitsgrundsätzen genügen (Rn. 216).
- Lange Verweisungsketten diverser Paragraphen aus verschiedenen Gesetzen müssen vermieden werden (Rn. 215).
- Wird bei einer Übermittlung der Zweck der Datenerhebung geändert, gilt das sogenannte Kriterium der hypothetischen Datenneuerhebung. Demnach "kommt es darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln neu erhoben werden dürften" (Rn. 216).

- Mit der strategischen Fernmeldeaufklärung steht dem BND ein besonders eingriffsintensives Überwachungsinstrument zur Verfügung, dessen Zweck vor allem final bestimmt ist: Er soll die Bundesregierung informieren und Gefahren frühzeitig erkennen – und das anlasslos, also gerade nicht durch im Vorhinein klar definierte Zwecke, sondern im Vergleich zur Strafverfolgung offeneren Befugnissen. Gerade weil der BND dadurch weit mehr Daten erheben kann als verfassungsrechtlich sonst zulässig, müssen die schärferen Vorschriften bei der Übermittlung gelten, um den Grundrechtsschutz auf dieser Ebene "verspätet" zu sichern (Rn. 218).
- Da der BND im Gegensatz zu anderen Sicherheitsbehörden gerade nicht die Daten für eigene "Ermittlungen" erhebt, können Übermittlungsschwellen entfallen, wenn der BND die Bundesregierung im Sinne der Auslandsaufklärung "nur" informiert (Rn. 223). Umso wichtiger ist daher, dass diese Daten nur für diesen Zweck verarbeitet werden.

Diese Anforderungen an die Übermittlung gelten für den BND immer, egal ob ins In- oder Ausland übermittelt werden soll, egal ob im Einzelfall oder durch automatisierte Kooperationen.

III.5.2 Übermittlung inländisch

Dass im "Kerngeschäft" des BND, nämlich der Auslandsaufklärung für die Bundesregierung, keine wesentlichen Übermittlungsschwellen gelten, heißt nicht, dass diese Tätigkeit der Kontrolle gänzlich entzogen werden sollte. Im Gegenteil: Das zentrale Argument des Bundesverfassungsgericht für die geringen Hürden bei Übermittlungen sind schließlich, dass "eine Zweckänderung insoweit prinzipiell ausgeschlossen ist und die durch solche Überwachungsmaßnahmen gewonnen Erkenntnisse (...) nicht an andere Stellen weitergeleitet werden dürfen" (Rn. 177). Der Bundesdatenschutzbeauftragte, vor allem aber der Kontrollrat müssen in ihrer Kontrolle zumindest stichprobenartig prüfen, dass Informationen aus der Bundesregierung nicht "auf dem kurzen Dienstweg" ohne gesetzliche Grundlage zu den Sicherheitsbehörden gelangen. Außerdem sollten sie zumindest stichprobenartig prüfen, inwiefern die Lageberichte des BND den verfassungsrechtlichen Anforderungen genügen, zum Beispiel indem dort möglichst keine identifizierbaren Informationen der überwachten Personen enthalten sind, um Repressalien möglichst auszuschließen (Rn. 225).

Eine besondere Herausforderung scheinen hierbei inländische Kooperationsprojekte zu sein, in denen die Grenzen zwischen Nachrichtendiensten, operativen Sicherheitsbehörden und Regierungsebene verschwimmen, zum

Beispiel im Gemeinsamen Terrorismusabwehrzentrum (GTAZ). Dort tauschen sich vorrangig Beamte von Sicherheitsbehörden aus, was im Sinne eines besseren Informationsaustausches zwischen den Behörden durchaus sinnvoll ist. Schon hier ist aber fraglich, ob es in den Diskussion eingehalten werden kann, dass der BND nur Informationen aus der Gefahrenfrüherkennung mitteilt, nicht jedoch aus der allgemeinen nachrichtendienstlichen Aufklärung. Dort nehmen beispielsweise mit dem Bundesamt für Migration und Flüchtlinge als Bundesoberbehörde des Innenministeriums jedoch auch Vertreter:innen der Bundesregierung teil. Hier wird immer wieder auch über konkrete Personen und deren Gefährdungspotential gesprochen.[15] Im Gesetzgebungsverfahren zur BND-Reform sollte daher auch erörtert werden, den Kontrollrat und den Bundesdatenschutzbeauftragten in solche Gremien standardmäßig zu entsenden und zumindest mit einem Hinweisrecht auf problematisch Datenübermittlungen auszustatten. Solche Einblicke in die "Praxis der Sicherheitsbehörden" sind unverzichtbar, um Kontrolllücken außerhalb des BND zu entdecken.

Anders sieht es aus, wenn Daten des BND, die zur Gefahrenfrüherkennung gewonnen worden sind, innerhalb Deutschlands an andere Sicherheitsbehörden übermittelt werden sollen. Hierfür gelten bereits im Genehmigungsverfahren bei Netzanordnungen und der Auswahl von Selektoren deutlich höhere Schwellen. Diese Datenerhebung muss unserem Vorschlag nach ex ante vom Kontrollrat genehmigt werden und kann im Grundsatz nur dafür verwendet werden, um Informationen für die zuvor genehmigten Zwecke zu sammeln und zu übermitteln. Ändert sich der Zweck, gilt hierfür das Prinzip der hypothetischen Datenneuerhebung. Gerade hierin muss künftig ein Kontrollschwerpunkt liegen: Jede Übermittlung – ob ohne oder mit hypothethischer Datenneuerhebung – sollte protokolliert werden müssen, um sie später einer Kontrolle zuführen zu können (Rn. 229). Es mag unpraktikabel und übertrieben erscheinen, Datenübermittlungen gerade im Bereich der Gefahrenfrüherkennungen unter Genehmigungsvorbehalt des Kontrollrats zu stellen. Umso wichtiger ist jedoch, dass die Kontrollorgane ex post nachvollziehen können, ob die Übermittlungspraktiken des BND den gesetzlichen Anforderungen genügen. Ist dem nicht so, braucht es Beanstandungsrechte und Sanktionsbefugnisse (siehe Kapitel IV 1.6).

Was aber, wenn bei der allgemeinen Auslandsaufklärung Erkenntnisse erlangt werden, die auch für die Gefahrenfrüherkennung relevant sein können? Das Urteil ist hier sehr deutlich. Eine Übermittlung scheidet in diesem Fall

15 Diese Praxis wurde in Bezug auf den Attentäter Anis Amri jüngst nochmal beschrieben in Diehl, Jörg, Lehberger, Roman, Schmid, Fidelius. 2020. Undercover. Ein V-Mann packt aus. DVA: München, S. 234 ff.

"prinzipiell aus" und ist "auch im Wege der regulären Zweckänderung nicht möglich" (Rn. 228). Dies bekräftigt nochmals die Notwendigkeit unseres Vorschlags, sowohl bei der Erhebung als auch der Verarbeitung von Daten organisatorisch, räumlich, personell und technisch getrennte Systeme für die allgemeine Auslandsaufklärung einerseits und die Gefahrenfrüherkennung andererseits aufzubauen (siehe Kapitel III.4). Eine Ausnahme davon sei laut Bundesverfassungsgericht nur möglich, soweit aus Daten der allgemeinen Auslandsaufklärung direkt eine "unmittelbar bevorstehende Gefahr" für das Leben von Menschen oder die Sicherheit von Bund und Ländern erkennbar werde. Es würde auch hier der Logik solcher Situationen widersprechen, eine ex ante-Kontrolle einzufordern. Dennoch muss eine solche Zweckänderung die absolute Ausnahme bleiben, weshalb zu fordern wäre, dass bei einer solchen Zweckänderung der Kontrollrat automatisch benachrichtigt würde und eine ex post-Genehmigung unverzüglich nachzuholen wäre.

III.5.3 Kooperation mit ausländischen Nachrichtendiensten

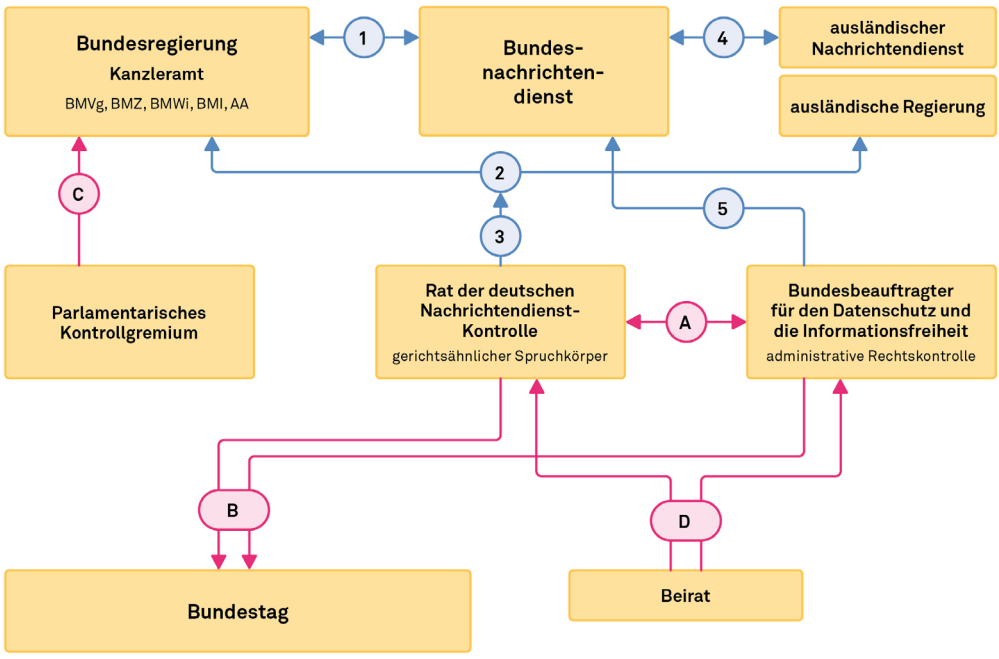
Noch einmal erhöhte Anforderungen haben in Zukunft zu gelten, wenn der Bundesnachrichtendienst selbst erhobene Daten mit ausländischen Nachrichtendiensten teilen möchte. Zwar erkennt das Bundesverfassungsgericht im Urteil die Notwendigkeit des "do ut des" nachrichtendienstlicher Tätigkeit grundsätzlich an. Allerdings müssen Bundesregierung und BND fortan de facto ausschließen können, dass mit ihren Daten verfassungsrechtlich verbürgte Schutzrechte – im Extremfall die Menschenwürdegarantie – im Empfängerstaat von Daten unterlaufen werden. Keine einfache Aufgabe, da der BND aktuell mit rund 450 Geheimdiensten weltweit kooperiert.

Unser Schaubild zeigt die Grundzüge eines künftigen Kooperationsverlaufs und die Einbettung der Kontrolle exemplarisch auf. Demnach kann entweder die Bundesregierung politisch eine Kooperation mit einer ausländischen Regierung anregen, oder der BND stößt im Rahmen seiner Tätigkeit auf die Notwendigkeit, mit ausländischen Nachrichtendiensten zu kooperieren. Ehe das losgehen kann, braucht es jedoch eine Kooperationsvereinbarung. Vergleichbares fordert auch bisher schon die Absichtserklärung gemäß § 13 Abs. 3 BND-Gesetz, doch die Anforderungen steigen in Zukunft deutlich. Zentrale Aspekte dieser "Rechtsstaatlichkeitsvergewisserung" müssen sein:

- Es braucht im Empfängerstaat Datenschutzgarantien im Sinne einer "Gewährleistung eines angemessenen materiellen datenschutzrechtlichen Niveaus für den Umgang mit den übermittelten Daten" (Rn. 236).
- Es muss "insbesondere gewährleistet erscheinen, dass die Informationen dort weder zu politischer Verfolgung noch zu unmenschlicher oder erniedrigender Bestrafung oder Behandlung (...) eingesetzt werden" (Rn. 237).

- Maßgeblich für die Bewertung dieser beiden Vergewisserungspflichten sind die Rechtsordnungen des Empfängerstaates. Gleichwohl muss sich der BND informieren, ob die Gesetze reine “Papiertiger” sind oder auch die Realität widerspiegeln (Rn. 238).
- Sollen Daten aus besonders schutzwürdigen Kommunikationsbeziehungen ins Ausland übermittelt werden, zum Beispiel über Journalistinnen und ihre Quellen, muss dies “grundsätzlich einer gerichtsähnlichen Vorabkontrolle unterliegen” (Rn. 240).
- Der BND muss seinerseits auf eine Third Party-Rule drängen, sodass die eigenen Daten vom ausländischen Partner nicht ohne Zustimmung des BND an einen weiteren ausländischen Staat weitergegeben werden (Rn. 242).

Kontrolle der Kooperation mit ausländischen Nachrichtendiensten



Verfahren pro Antrag

1. Aufklärungs- und Kooperationsinteresse mit ausländischen Regierungen und ihren Nachrichtendiensten
2. Kooperationsvereinbarung und Rechtsstaatlichkeitsvergewisserung
3. *ex ante*-Kontrolle der Kooperationsvereinbarung und Rechtsstaatlichkeitsvergewisserung
4. gegenseitiger Austausch von Daten
5. Kontrolle der gegenseitigen Übermittlung von Daten sowie der Datenverarbeitung beim BND

Kontrollvorgaben

- A: regelmäßiger Austausch der jeweiligen Kontrollergebnisse bezüglich internationaler Kooperationen deutscher Nachrichtendienste
- B: Bericht an den Bundestag über Kontrolltätigkeit
- C: anlassbezogene politische und finanzielle Kontrolle sowie politische Kontrolle ausgewählter Absichtserklärungen
- D: ständige Beratung, z.B. zu technischer Entwicklung oder Menschenrechtssituation in bestimmten Ländern

Unserem Vorschlag nach sollte der Kontrollrat sämtliche Rechtstaatlichkeitsvergewisserungen vor Inkrafttreten gerichtsähnlich prüfen. Sie müssen genehmigt werden, ehe sie die Bundesregierung zur Kooperation ermächtigen. Eine Ausnahmemöglichkeit für etwaige "Eilverfahren" ist hier nicht geboten, da die Rechtsstaatlichkeitsvergewisserungen erst die Möglichkeit eröffnen, in Zukunft von solchen "Eilfällen" gegenseitig erfahren zu können. Der Kontrollrat muss also bevor Daten ausgetauscht werden erst prüfen, ob die allgemeinen Voraussetzungen im Empfängerstaat dafür gegeben sind. Es sollte nicht erforderlich sein, dass der Kontrollrat den gesamten Vertrag nochmals nachrecherchiert und in jeder Einzelheit auf Plausibilität prüft. Aber er sollte in begründeten Fällen die Möglichkeit haben, es zu tun.

Der Kontrollrat muss hierfür eigene Kompetenzen aufbauen, um beispielsweise selbst Kriterien für den Vergleich unterschiedlicher Datenschutz-Regime zu entwickeln. Gerade für solche Fragen sehen wir den Beirat als wichtige Anlaufstelle für den Kontrollrat: Fern ab von Einzelfällen, die aufgrund von Geheimhaltungspflichten ohnehin nicht erörtert werden könnten, können hier gerade solche Methoden des internationalen Rechtsvergleichs oder Informationen zur Menschenrechtssituation in bestimmten Ländern von den Expertinnen und Experten zugeliefert werden.

III.5.3.1 Übermittlung im Einzelfall ins Ausland

Erst wenn die Rechtstaatlichkeitsvergewisserung genehmigt worden ist, kann der Datenaustausch zwischen BND und ausländischem Nachrichtendienst losgehen. In der täglichen Arbeit wird dann die Rolle des Bundesdatenschutzbeauftragten bedeutender, da dieser für die administrative Rechtskontrolle zuständig ist. Dies gilt auch für die Verarbeitung von Daten durch den BND, die aus dem Ausland stammen. Auch der Kontrollrat sollte jedoch zumindest stichprobenartig, zum Beispiel im Rahmen gemeinsamer Kontrollbesuche mit dem BfDI, den Grundrechtsschutz in der Praxis überprüfen. Dies macht es erforderlich, dass sowohl der Kontrollrat als auch der BfDI in der Kooperationsvereinbarung nicht als Third Party definiert werden. Sie müssen Zugriff auf die zwischenstaatlichen Verträge ebenso wie auf die Datenverarbeitung haben (Rn. 292).

Bei der Frage, welche Informationen der BND ins Ausland übermittelt, kommen von vornherein nur diejenigen in Betracht, die im Rahmen der Gefahrenfrüherkennung erlangt worden sind – also bei dem Teil der strategischen Kommunikationsüberwachung, der bereits bei Erhebung und Verarbeitung an klare Zwecke geknüpft werden muss (Rn. 177). Für die Kontrollpraxis wird einmal mehr entscheidend sein, dass Übermittlungen protokolliert werden. Dadurch kann ersichtlich werden, ob die Zweckbindung auch bei ausländi-

schen Kooperationen gewahrt bleibt. Dies scheint besonders in diesem Fall entscheidend, weil die Betroffenen hier ein hohes Risiko laufen, in anderen Ländern Ziel von Ermittlungen zu werden. Eine Sonderrolle für den Kontrollrat gibt es ferner bei der Überwachung besonders schutzwürdiger Kommunikationsbeziehung wie zum Beispiel von Anwält:innen mit ihrer Mandantschaft: Hier müssen Übermittlungen "grundsätzlich einer gerichtsähnlichen Vorabkontrolle unterliegen" (Rn. 240).

III.5.3.2 Automatisierte Kooperationen

Bei automatisierten Kooperationen öffnet der BND Schnittstellen zum eigenen Rohdatenstrom, in dem ausländische Nachrichtendienste dann eigene Selektoren als Filter steuern. Es ist auch möglich, dass Metadaten automatisiert ins Ausland weitergeleitet werden, damit diese dort analysiert und gegebenenfalls auf Vorrat gespeichert werden können. Der BND stellt dabei gewissermaßen die Infrastruktur für die Überwachung anderer bereit.

Bundesregierung und BND wurden bei der mündlichen Verhandlung recht schmallippig als es darum ging, inwiefern bei automatisierten Kooperationen mit ausländischen Nachrichtendiensten ein Missbrauch ausgeschlossen werden könne. Der BND gibt schließlich die Zügel aus der Hand und verlässt sich, so die Aussagen der Beteiligten, auf die Absichtserklärungen und eigene Stichproben. Auch dies muss sich in Zukunft ändern.

Für den Fall, dass ausländische Nachrichtendienste ihre Selektoren an den BND übermitteln und die Ergebnisse automatisiert erhalten, kommt einer automatisierten Kontrolle besondere Bedeutung zu – also insbesondere die Filterverfahren und die Prüfung der ausländischen Selektoren. Wir schlagen vor, dass der BND die eigenen Filtersysteme 1:1 auch anwendet, bevor er die Rohdaten für die Selektoren des ausländischen Partners freigibt. Es ist nicht ersichtlich, warum andere Nachrichtendienste unter Mithilfe des BND etwas überwachen können dürfen, das dem BND verfassungsrechtlich nicht erlaubt wäre. Besonders wichtig sind entsprechend eine G10-Filterung, um eine Inlandsüberwachung durch ausländische Nachrichtendienste zu verhindern (siehe Kapitel III.2 und III.3). Auszuschließen ist vor allem ein sogenannter "Ringtausch", indem Nachrichtendienste vom Gegenüber Daten erhalten, die sie selbst nicht hätten erheben dürfen (Rn. 248).

Hohe Bedeutung hat ebenfalls der Einsatz von Schutzlisten als Filter, ehe ausländische Nachrichtendienste darauf zugreifen können. Auf diesen Listen stehen beispielsweise die Telefonnummern von Journalist:innen, die in ihrer Kommunikation mit Quellen besonders auf Vertraulichkeit angewiesen sind (siehe III.3). Gerade in Staaten mit schwachem rechtsstaatlichen Struk-

turen drohen Angehörigen dieser Berufsgruppen auch physische Gefahren wie Freiheitsentzug oder gar Folter. Der BND muss diese Schutzlisten daher auch als Filter für ausländische Selektoren einsetzen (Rn. 258) und, besser noch, als rote Linie der automatisierten Kooperationen überhaupt betrachten. Zwar gilt der Schutz dieser Berufsgruppen bei selektorengestützer Überwachung nicht ohne Einschränkungen. Dennoch sollte aufgrund der Schutzwürdigkeit dieser Berufsgruppen eine Überwachung hier die Ausnahme sein, was mit einer automatisierten Übernahme ausländischer Selektoren kaum vereinbar scheint. Wenn tatsächlich ein überragendes Interesse an einer Überwachung dieser Personen durch ausländische Stellen besteht, sollten die Selektoren menschlich geprüft und vom Kontrollrat ex ante, und danach kontinuierlich erneut genehmigt werden müssen.

Erst wenn diese Filterstufen durchlaufen sind, kommt eine Arbeit des ausländischen Nachrichtendienstes mit den Rohdaten des BND in Betracht. Zwar können Selektoren dann "automatisiert" gesteuert werden, doch auch diese Selektoren müssen vorab ebenfalls daraufhin geprüft werden, dass die verfassungsrechtlichen Vorgaben nicht umgehen (Rn. 255). Diese Prüfung mag aufgrund ihrer Menge nur durch den BND zu leisten sein, doch sie müssen einer unabhängigen Kontrolle durch Kontrollrat und BfDI grundsätzlich offen stehen. Der Kontrollrat sollte außerdem das Recht haben, die Verwendung von Selektoren – wie schon bei durch den BND bestimmten Selektoren – zu untersagen.

Andere Kontrollvorgaben gelten, wenn der Bundesnachrichtendienst in Zukunft den ausländischen Partnerdiensten "seinen" Rohdatenstrom ungeprüft ausleiten will. Anders als im zuvor beschriebenen Fall sieht der BND nicht einmal mehr, was der ausländische Dienst mit den Daten macht, sondern er leitet Rohdaten einfach weiter. Karlsruhe verlangt hierfür, dass die kooperierenden Geheimdienste benennen können müssen, warum dies für bestimmte Netze erforderlich ist, weil in bestimmten Weltregionen eine "spezifisch konkretisierte Gefahrenlage" vorliegt, zum Beispiel illegaler Waffenhandel von Terroristen. "Eine gesamthafte Übermittlung von Verkehrsdaten kann nicht kontinuierlich und allein final angeleitet erlaubt werden" (Rn. 263).

Der Kern dieser Art von Kooperation ist es, die Metadaten von Kommunikation weiterzuleiten – also zum Beispiel wer wann mit wem über welchen Kanal kommuniziert, aber eben nicht was genau. Solche Verkehrsdaten sind gleichermaßen an Artikel 10 GG zu messen, weil sie die Umstände von Telekommunikation detailliert beschreiben können: Für Journalist:innen zum Beispiel sind solche Metadaten besonders sensibel, denn wenn bekannt ist,

dass eine Redaktion mit einer potentiellen Quelle in Kontakt stand und kurz darauf eine Story mit Insiderwissen veröffentlicht, muss ein:e Überwacher:in nicht mehr wissen, was konkret gesprochen worden ist. Beachtenswert ist folglich, dass Karlsruhe zum einzigen Mal im Urteil den Schutz bestimmter Berufsgruppen bei der automatisierten Ausleitung von Metadaten absolut gesetzt hat (Rn. 264). Gleiches gilt für Verkehrsdaten deutscher Personen. Der BND kann in Zukunft also nur Metadaten ins Ausland weiterleiten, wenn darin die Filter für den G10-Schutz sowie die für geschützte Berufsgruppen absolut angewendet worden sind. Außerdem braucht es die Zusicherung, dass die Verkehrsdaten spätestens nach sechs Monaten vom Partnerdienst gelöscht werden (Rn. 264).

Da die "Arbeit" mit den Daten bei solchen Kooperationsformen im Ausland stattfindet, ist die Kontrolltätigkeit von Kontrollrat und BfDI von vornherein eingeschränkt. Umso wichtiger wird sein, die Einhaltung der "absoluten Filterung" vor Weiterleitung ins Ausland kontinuierlich zu kontrollieren und auch zu optimieren. Während hier vor allem der Bundesdatenschutzbeauftragte im Rahmen der administrativen Rechtskontrolle gefragt sein wird, kommt dem Kontrollrat die Aufgabe zu, die "gehaltvollen Zusagen" (Rn. 259) ausländischer Nachrichtendienste in puncto Plausibilität und Aktualität stichprobenartig zu überprüfen und bei Zweifeln ein Beanstandungsrecht gegenüber der Bundesregierung ausüben zu können.

III.6 Zwischenfazit: neue Dimension der Kontrolldichte

Die vorangegangene Analyse dessen, was das Bundesverfassungsgericht an Auflagen für das Verfahren der strategischen Fernmeldeaufklärung nennt, zeigt: die Kontrolldichte und Prüfintensität muss sich in Zukunft enorm steigern. Wenn die Bundesregierung am Instrument der massenhaften Datenauswertung durch den Bundesnachrichtendienst festhalten will, muss in den verschiedenen Phasen der Überwachung eine unabhängige Kontrolle gewährleistet werden.

Wir haben dies anhand unseres Vorschlags eines dreigliedrigen Kontrollgefüges, bestehend aus PKGr, Kontrollrat und BfDI, aufgezeigt, doch selbst wenn sich der Gesetzgeber für einen anderen Weg entscheidet, sind die verfassungsrechtlich gebotenen Anforderungen zu adressieren. Die deutsche Nachrichtendienst-Kontrolle der Zukunft braucht deutlich mehr Befugnisse, Ressourcen und Technologien, um ihrer Aufgabe gerecht werden zu können. Was dies im Einzelnen heißt, erörtern wir im folgenden Kapitel IV.

IV. Folgen für die Kontrollpraxis

Das Bundesverfassungsgericht hat mit diesem Grundsatzurteil das bisherige Primat der parlamentarischen Aufsicht bei der Kontrolle des Bundesnachrichtendienstes aufgehoben. Um die durch die Digitalisierung gestiegene Macht des Auslandsnachrichtendienst wirksam zu kontrollieren, bedarf es zudem einer deutlich gestärkten Rechtskontrolle. Zukünftig sollten nicht (mehr), wie vom PKGr-Vorsitzenden Armin Schuster in der mündlichen Verhandlung behauptet, "alle Fäden beim PKGr zusammenlaufen". Anforderungen zur Ausgestaltung der parlamentarischen Kontrolle "lassen sich aus den in vorliegendem Verfahren geltend gemachten Grundrechten nicht ableiten" (Rn. 300).

IV.1 Besetzung, Befugnisse und Pflichten der Rechtskontrolle

Um bei der Neustrukturierung der Kontrolle den Vorgaben des Bundesverfassungsgerichts gerecht zu werden, schlagen wir unter anderem eine Auflösung des Unabhängigen Gremiums in Karlsruhe vor. Dennoch sollten bei der Reform die Verdienste einzelner Mitarbeiter:innen des Unabhängigen Gremiums nicht vergessen werden.[16] Die Schaffung des Unabhängigen Gremiums hat insbesondere Impulse dafür gegeben, mit welchem Personal ein Kontrollrat besetzt werden sollte, welche Befugnisse er benötigt und welche Ressourcen in personeller und technologischer Hinsicht wichtig sind.

IV.1.1 Besetzung des Kontrollrats

Im Genehmigungsverfahren sind der Spürsinn und die Unabhängigkeit eines Ermittlungsrichters bzw. einer Ermittlungsrichterin gefragt. Den Vorsitz des Unabhängigen Gremium haben derzeit zwei Richter:innen des Bundesgerichtshofs inne. Diese oder vergleichbare Kriterien für die Mitgliedschaft des gerichtsähnlichen Kontrollrats – anders als gegenwärtig der Fall für die Mitgliedschaft in der G10-Kommission – sollten beibehalten und gesetzlich konkretisiert werden. Mindestanforderungen an eine Mitgliedschaft sollten dabei nicht nur für den Vorsitz gelten, sondern auch für die zahlreichen neu-

16 Diese kamen besonders klar während der mündlichen Verhandlung im Januar 2020 zum Ausdruck. Den für einen zukünftigen Spruchkörper wichtigen ermittlerischen Spürsinn hat das Unabhängige Gremium beispielsweise bewiesen, indem es bei der Frage welche Angaben in ein von ihr auf Zulässigkeit und Notwendigkeit zu prüfenden Anordnung enthalten sein müssen sich nicht mit pauschalen Informationen zufrieden gab und nachbohrte. Das betraf beispielsweise Informationen zu Grund und Dauer einer Maßnahme, das betroffene Telekommunikationsnetz und die verpflichteten Unternehmen. Hier hat das Gremium stetig um statische Angaben zu Meldeaufkommen gebeten, um diese auch in ihrer zeitlichen Entwicklung einordnen zu können. Anders als vermutlich vom Bundeskanzleramt erhofft, lag dem Prüfverhalten des UGr eine unterschiedliche Interpretationen der "Stichprobenkontrollbefugnis" zugrunde, die einen regen Briefwechsel zu Folge hatte.

en Stellen, die erst noch besetzt werden müssen. Ein Festhalten am Ehrenamt, dies hat Karlsruhe klar festgestellt, wird nicht mehr möglich sein (Rn. 287). Stattdessen gilt es, eine Vielzahl an Kontrolleur:innen hauptamtlich zu berufen. Auf Leitungsebene müssen sowohl beim Kontrollrat als auch beim Bundesdatenschutzbeauftragten Stellen geschaffen werden, die hohen technischen Sachverstand in den Bereichen IT, Sicherheitsrecht, IT-Recht, Verwaltungsrecht und Sicherheitspolitik besitzen.

IV.1.2 Kontrollbefugnisse

Bezüglich der Befugnisse des Spruchkörpers hat Karlsruhe klargestellt, dass zukünftig folgende Verfahrensschritte grundsätzlich einer gerichtsähnlichen Kontrolle mit abschließenden Entscheidungsbefugnissen zu unterliegen haben:

- die "formalisierte Festlegung der verschiedenen Überwachungsmaßnahmen, auch im Bereich der Kooperationen, die konkrete Netzanodnungen, der Einsatz von Suchbegriffen, soweit diese gezielt auf Personen gerichtet sind, welche als mögliche Gefahrenquelle im unmittelbaren Interesse des Nachrichtendienstes stehen,
- der Einsatz von Suchbegriffen, die gezielt auf Personen gerichtet sind, deren Kommunikation einen besonderen Vertraulichkeitsschutz genießt, die zum Schutz solcher Vertraulichkeitsbeziehungen erforderlichen Abwä- gungsentscheidungen,
- der Umgang mit Daten, die möglicherweise dem Kernbereich privater Lebensgestaltung unterfallen,
- besonders kontrollbedürftige Übermittlungen, vor allem an ausländische Stellen, sowie die Voraussetzungen für die Festlegung einer Zusammenarbeit zur automatisierten Übermittlung von Verkehrsdaten zur bevorratenden Speicherung und Auswertung an ausländische Dienste.
- die ausnahmsweise Nutzung von Daten unter Berufung auf besondere Gefahrensituationen, obwohl es sich um – erst in der manuellen Auswertung erkannte – Daten aus Telekommunikation unter Beteiligung von Deutschen oder Inländern handelt oder die Daten aus Überwachungsmaßnahmen stammen, die sich nicht auf Zwecke der Gefahrenfrüherkennung stützten, sondern unabhängig davon allein zur politischen Information der Bundesregierung angeordnet waren." (Rn. 278)

Im Zuge der Reform ist gesetzlich sicherzustellen, dass Kontrollrat und BfDI die nötigen rechtlichen Befugnisse und technischen Zugänge erhalten, um diesen verfassungsrechtlichen Kontrollauftrag angemessen wahrnehmen zu können.

IV.1.3 Protokollierungspflichten

Auch zu den Protokollierungspflichten haben die Verfassungsrichter:innen detaillierte Vorgaben gemacht, was dem Ziel einer datenbasierten Nachrichtendienst-Kontrolle entgegenkommt. Sie fordern insgesamt, dass zu den verfassungsrechtlichen Anforderungen in Hinblick auf die Kontrolle "eine Protokollierung der Datenverarbeitung [gehört]. Danach müssen die verschiedenen Schritte der Überwachung in einer Weise protokolliert werden, die eine wirksame Kontrolle ermöglicht." (Rn. 291). Dies beinhaltet beispielsweise auch: "Löschungsprotokolle müssen zur Gewährleistung einer datenschutzrechtlichen Kontrolle hinreichend lang aufbewahrt werden" (Rn. 207). Protokollierungspflichten greifen auch beim Einsatz von Filtermethoden. Hier ist gesetzlich sicherzustellen, dass "dann, wenn im Rahmen der weiteren Auswertung Telekommunikationsdaten von Deutschen oder Inländern identifiziert werden, diese nicht genutzt werden dürfen und unverzüglich zu löschen sind. Zur Begründung einer solchen Befugnis reichen dienstinterne Hinweise auf allgemeine strafrechtliche Grundsätze nicht aus" (Rn. 174). Wird solche Kommunikation trotzdem genutzt, sollte dies in Zukunft protokolliert werden und bedarf einer gerichtsähnlichen Kontrolle (Rn. 174).

Da auch der BND selbst ein Interesse an Protokollierung hat, sollten in Zukunft die Bedürfnisse von BND und Kontrollorganen schon bei der Konzeption neuer Systeme berücksichtigt werden. Protokolldateien werden schließlich ohnehin für andere Zwecke als die Kontrolle im Nachrichtendienstwesen genutzt. Protokolldateien und andere relevante Daten sollten bei den Diensten so zu führen und zu pflegen sein, dass sie den Bedürfnissen der Rechtskontrolle entsprechen, um gerade auch die Arbeit der administrativen Rechtskontrolle durch den Bundesdatenschutzbeauftragten gerecht zu werden.

IV.1.4 Kontrolle von Analysesystemen und Algorithmen

Die Dimension der überwachten Daten im Rahmen der strategischen Fernmeldeaufklärung steigt qualitativ und quantitativ kontinuierlich an. Die Maßnahme ist mit denen früherer Entscheidungen des Bundesverfassungsgerichts "in ihrer Eingriffsintensität nicht mehr zu vergleichen. (...) Insgesamt erstreckt sich die strategische Telekommunikationsüberwachung damit inzwischen potentiell auf annähernd die gesamte Kommunikation auch der Zivilgesellschaft" (Rn. 151). Mit zunehmender Digitalisierung – man denke nur an das Internet der Dinge – wird diese Entwicklung eher zu- als abnehmen. Dies öffnet neue Gefährdungen für Grundrechte, stellt jedoch auch die Sicherheitsbehörden selbst vor neue Herausforderungen: Irgendwie müssen die erfassten Daten schließlich ausgewertet werden, ohne im Strom der Daten die Übersicht zu verlieren.

Die Bedeutung datengestützter Analyse- und Prognosesysteme wird in Zukunft steigen. Was in der Polizeiarbeit beispielsweise unter dem Stichwort des "Predictive Policing" diskutiert wird, gewinnt auch für einen Nachrichtendienst an Bedeutung, der unter anderem für die "Gefahrenfrüherkennung" zuständig ist. Erinnert sei nochmals daran, dass der BND aktuell allein am Internetaustauschknoten DE-CIX bis zu 1,2 Billionen Internetverbindungen pro Tag erfassen kann. Karlsruhe sieht auch hier den Bedarf einer Kontrolle: "Zu regeln ist gegebenenfalls auch der Einsatz von Algorithmen, insbesondere die Sicherstellung ihrer Grundsätzlichen Nachvollziehbarkeit in Blick auf eine unabhängige Kontrolle." (Rn. 192)

Insbesondere der Bundesdatenschutzbeauftragte muss in der Prüfung von Analysesystemen und eingesetzten Algorithmen einen Schwerpunkt für die administrative Rechtskontrolle bilden. Es geht insbesondere darum, eine Diskriminierung bestimmter Bevölkerungsgruppen zu verhindern. Diese Gefahr ist real und aus der Polizeiarbeit bekannt, wenn zum Beispiel Menschen allein aufgrund ihrer Nationalität, ihrer Hautfarbe oder ihres Wohnorts eine höhere Wahrscheinlichkeit attestiert wird – und es dadurch wahrscheinlicher wird, Ziel von staatlichen Ermittlungsmaßnahmen zu werden.[17] Der BfDI sollte hier im engen Austausch mit dem Kontrollrat stehen und gemeinsame Kontrollkriterien entwickeln, um die technischen mit den grundrechtlichen Prüfungen zu verzahnen. Beide müssen dafür uneingeschränkte Zugänge zu den Systemen inklusive der Trainingsdaten, Protokolldaten und des Quellcodes erhalten

In diesem Bereich sehen wir auch ein wichtiges Beratungsfeld des Beirats. Die Diskussion um die "Diskriminierung durch Algorithmen" ist ein in akademischen Zirkeln breit diskutiertes Thema. BfDI und Kontrollrat sollten diese Expertise nutzen und eigene Frage formulieren, die für ihre Kontrolltätigkeit drängend sind. Neben der "Diskriminierung durch Algorithmen" könnte ein weiteres "Zukunftsthema" sein, wie sich in präemptiven Prognosesystemen ein Grundrechtsschutz besonders schützenswerter Berufsgruppen technisch abbilden lassen könnte. Für den Journalismus ist beispielsweise besonders entscheidend, dass solche Systeme nicht dahingehend entwickelt werden, prognostizieren zu können, wer Quellen für Journalist:innen sein könnten – und staatliche Stellen präventiv Leaks verhindern, ehe sie eine Redaktion überhaupt erreichen.[18]

17 Knobloch, Tobias. 2018. Vor die Lage kommen: Predictive Policing in Deutschland. Stiftung Neue Verantwortung: Berlin, abrufbar unter: https://www.stiftung-nv.de/de/publikation/vor-die-lage-kommen-predictive-policing-deutschland

18 Theoretisch inspirierend hierfür: Esposito, Elena 2007. Die Fiktion der wahrscheinlichen Realität. Frankfurt am Main: Suhrkamp.

IV.1.5 Detaillierte Berichtspflichten

Eine öffentliche, informierte Diskussion ist eine demokratische Notwendigkeit für Vertrauen in die Arbeit staatlicher Stellen. Sie eröffnet erst die Möglichkeit, über Sinn und Nutzen von Überwachungsmaßnahmen zu entscheiden. Daher ist es im Rahmen des möglicherweise gebotenen 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. Gemäß unseres Vorschlags würden die drei zentralen Säulen der Nachrichtendienst-Kontrolle sowie der Beirat eigenständige Berichte verfassen. Im Folgenden wollen wir uns insbesondere auf die Berichte der beiden Instanzen der Rechtskontrolle – Kontrollrat und BfDI – fokussieren.
Anders als bei der G10-Kommission, die keine eigene Berichtspflicht hat und gemäß §14 Abs. 1 S.1 Art. 10 Gesetz das für die Beschränkungsmaßnahmen zuständige Bundesministerium das PKGr über Beschränkungsmaßnahmen unterrichtet, würden wir dem Kontrollrat eine Berichtspflicht auferlegen, damit dieser selbständig einen umfassenden Tätigkeitsbericht verfassen kann – und dabei nicht auf von den Ministerien vorformulierte Textbausteine zurückgreifen muss. Dies knüpft an Vorgaben an, wie sie übrigens auch in den Niederlanden und Großbritannien längst Standard sind. Der Tätigkeitsbericht des Kontrollrats sollte in regelmäßigen Abständen, mindestens jährlich, der Öffentlichkeit einen 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.

Warum das sinnvoll ist, zeigt der Blick auf andere Länder. In den Niederlanden hat das für die Genehmigungen von Überwachungsmaßnahmen zuständige Gremium TIB in seinem auch auf Englisch veröffentlichten Report kürzlich berichtet, dass es “in der Zeit vom 1. Mai 2018 bis zum 1. April 2019 insgesamt 2.159 Anträge” geprüft habe.[19] 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 unrechtmäßig befunden und abgelehnt wurden.

19 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

So wurde in

- 37 Fällen der Einsatz einer Maßnahmen für nicht notwendig befunden;
- 58 Fällen der Einsatz einer Maßnahme als unverhältnismäßig erachtet;
- 48 Fällen befunden, dass der Zweck der Maßnahme auch mit weniger invasiven Mittel hätte erreicht werden können;
- 68 Fälle befunden, dass dem Antrag für eine Maßnahme ausreichende Informationen über die relevante Tatsachen, nähere Umstände sowie Ausführungen über technische Risiken fehlten;
- 26 Fällen entschieden, dass eine unzureichende rechtliche Grundlage für die beantragte Maßnahme vorlag;
- 21 Fällen entschieden, dass eine beantragte Maßnahme den Geltungsbereich des Gesetzes überschritten hatte.

Zudem erörter der Bericht des TIB Beispiele für 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. Wie am niederländischen Beispiel verdeutlicht, ist dies möglich ohne dabei schützenswerte Informationen über den Auslandsnachrichtendienst und seine Arbeitsweisen preiszugeben. Wichtig wäre auch die Anzahl der Eilverfahren (ex post) mit dem standardmäßigen Genehmigungsverfahren (ex ante) in Bezug zu setzen, um zu erkennen, wie häufig von der Regel abgewichen wurde. Zudem sollten die Berichte über den Datenaustausch mit anderen deutschen Sicherheitsbehörden und gegebenenfalls auch über die Einbindung des Kontrollrats in die wachsende Kontroll-Kooperation europäischer Aufsichtsgremien informieren.

Der Bundedatenschutzbeauftragte sendet seinen Tätigkeitsbericht direkt an den Bundestag. Da der BfDI gemäß unseres Vorschlages künftig die gesamte administrative Rechtskontrolle für die Fernmeldeaufklärung übernimmt, sollte diese Kontrolltätigkeit einem besonderen Bericht, mindestens jedoch in einem deutlich umfassenderen Teil des BfDI Gesamtberichts, aufgeführt werden. Auch hier sollte der Bericht der Öffentlichkeit ein gehaltvolles Bild über die vielen laufenden Prüfverfahren und den Einsatz der Kontrolltechnik und die Ergebnisse von Inspektionen vermitteln. Darüber hinaus sollte der BfDI informieren, wie häufig der unzureichende Schutz vertrauenswürdiger Kommunikation etwa von Journalist:innen und Anwält:innen gegenüber dem Kontrollrat und dem Bundesnachrichtendienstes beanstandet wurde.

Der Tätigkeitsbericht sollte auch hinreichend Informationen über den Prozess und die Ergebnisse der Evaluationen der Datenminimierung und der Einhaltung zahlreicher Schutznormen beinhalten. Hier empfiehlt sich die Praxis des britischen Aufsichtsgremiums IPCO. In seinen Jahresberichten werden Prüfergebnisse an Empfehlungen geknüpft und diese sind mit farblicher Markierung je nach Dringlichkeit aufgeführt.[20]

So unterscheidet IPCO seinem Bericht zufolge zwischen Prüfergebnissen, die einer unmittelbaren Korrektur bzw. Handlung bei den Diensten oder der Regierung erfordern (rote Markierung) von Bereichen oder Aspekten, die zukünftig überarbeitet und angepasst werden sollten (gelbe Markierung). Zudem werden Verbesserungen vorgeschlagen, um in einem frühen Stadium zu verhindern, dass zukünftig Probleme der Nichteinhaltung eintreten oder wo Effizienzsteigerungen erzielt werden könnten oder wo für eine Beurteilung zusätzliche Informationen erforderlich sind (grüne Markierung).

Der Bericht des Bundesdatenschutzbeauftragten sollte auch über dessen Beanstandungen und ggf. Sanktionen informieren.

IV.1.6 Sanktionsmöglichkeiten

Ohne androhbare und auch umsetzbare Konsequenzen hat die administrative Rechtskontrolle wenig Durchsetzungskraft. Die Reform sollte von daher auch Sanktionsbefugnisse für die beiden Organe der Rechtskontrolle (Kontrollrat, BfDI) beinhalten, damit etwaige Rechtsverstöße auch Folgen für die Nachrichtendienste bzw. die Bundesregierung haben. Bisher fehlen solche Möglichkeit fast völlig. Auch hier bieten das geltende Nachrichtendienstrecht anderer Demokratien bzw. Analogien zu EU-Richtlinien interessante Ansatzpunkte für die anstehende Reform in Deutschland.

IV.1.6.1 Bei Behinderung oder Missachtung von Kontrollvorgaben

In Norwegen ist gesetzlich festgelegt, dass die Missachtung von Anfragen der Kontrollgremien strafrechtlich sanktioniert werden kann. Amtierende oder ehemals Beschäftigte eines norwegischen Nachrichtendienstes sind verpflichtet, Anfragen zu beantworten und allen Aufforderungen der Kontrollbehörde nachzukommen – und zwar unabhängig vom Geheimhaltungsgrad. “Vorsätzliche oder grob fahrlässige Verstöße” gegen diese Pflicht führen dazu, dass “eine Geldstrafe oder eine Freiheitsstrafe von höchstens

20 siehe PCO Jahresbericht 2018, abrufbar unter: https://ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf

einem Jahr verhängt wird, sofern nicht strengere strafrechtliche Bestimmungen gelten".[21]

IV.1.6.2 Bei Missachtung datenschutzrechtlicher Vorgaben

Da die EU keine Gesetzgebungskompetenz im Bereich der Nachrichtendienste hat, steht eine direkte Umsetzung der hiernach zitierten EU-Richtlinie in das Nachrichtendienstrecht der Bundesrepublik Deutschland nicht im Raum. Gleichwohl ließen sich in Anlehnung an diese Richtlinie Forderungen für die Neufassung der Nachrichtendienstgesetze ableiten. Gemäß der EU-Richtlinie[22] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden kann die Datenschutzbehörde bestimmte Datennutzung untersagen. Dementsprechend haben nach Art. 47 Abs. 2 dieser Richtlinie die Mitgliedstaaten mittels eigener Rechtsvorschriften unter anderem vorzusehen, "dass jede Aufsichtsbehörde über wirksame Abhilfe-Befugnisse (...) verfügt, die es ihr gestatten, (...) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen." Dies würde zwar über das von den Karlsruher Richtern geforderte Beanstandungsrecht (Rn. 276) der administrativen Rechtskontrolle hinausgehen, könnte im Zusammenwirken mit dem gerichtsähnlichen Spruchkörper aber in eine neue Sanktionsmöglichkeit münden.

IV.1.7 Benachrichtigungen

Obwohl es die strategische Fernmeldeaufklärung als breit angelegte Überwachungsmethode besonders wahrscheinlich macht, dass auch die Kommunikation unbescholtener Menschen erfasst und ausgewertet wird, erfahren die Betroffenen praktisch nie davon. Rechtfertigung hierfür ist Art. 10 Abs. 2 S. 2 GG, wonach die Benachrichtigungspflicht bei Überwachungsmaßnahmen entfallen kann, wenn diese "der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes dient" und "an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt". Diese Ausnahme ist bei der strategischen Telekommunikationsüberwachung seit Jahrzehnten die Regel – und auch hier hat das Bundesverfassungsgericht Verbesserungen angemahnt.

---

21 Norwegisches EOS-Kontrollgesetz, Abschnitt 21 - siehe englische Übersetzung auf S. 82 des EOS Annual Reports: https://eos-utvalget.no/wp-content/uploads/2019/05/eos_annual_report_2018.pdf

22 EU-Richtlinie 2016/680 des Europäischen Parlamentes zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016L0680&from=DE#d1e2712-89-1

Zu den Anforderungen an die verfassungsmäßige Überwachung aller Sicherheitsbehörden “gehören weiterhin grundsätzlich Benachrichtigungspflichten” (Rn. 267). Zwar können diese gerade bei der strategischen Überwachung massiv eingeschränkt werden, aber es bleibt dabei, dass die Nicht-Benachrichtigung zu begründen ist und nicht andersherum. Dies ist ein demokratisches Grunderfordernis, um Betroffenen den Rechtsweg zu eröffnen. Bei der Frage, welche Menschen das höchste Interesse an einer Benachrichtigung haben, sollte sowohl anhand der Staatsangehörigkeit als auch funktional nach ihrer Betroffenheit von Überwachung differenziert werden.

Ein grundsätzliches Recht auf Benachrichtigungen haben Deutsche oder in Deutschland lebende ausländische Personen, weil sie aufgrund der territorialen Nähe zur deutschen Staatsgewalt stärker gefährdet sind, Ziel weiterer Ermittlungen und Grundrechtsbeschränkungen aufgrund der Überwachungsmaßnahmen zu werden. Sie sollten gemäß dem Urteil immer dann benachrichtigt werden, wenn ihre Überwachung von den technischen Filtermechanismen nicht erkannt und erst bei der menschlichen Auswertung bemerkt worden ist (Rn. 268). Diese G10-Benachrichtigungspflicht sollte gesetzlich in der Reform berücksichtigt und ein Schwerpunkt des Kontrollrats werden.

Bei ausländischen Personen im Ausland hingegen kann der Gesetzgeber zwar “grundsätzlich von Benachrichtigungspflichten absehen” (Rn. 269). Wir plädieren jedoch dafür, zumindest für EU-Bürger:innen Benachrichtigungspflichten einzuführen, denn mit dem voranschreitenden Ausbau der “Security Union” innerhalb der EU intensiviert sich der intraeuropäische Datenaustausch zwischen den EU-Behörden. Dies erhöht wiederum die Gefahr für EU-Bürger:innen, nach Überwachungsmaßnahmen Ziel von Ermittlungsmaßnahmen zu werden.

Allein auf die Staatsangehörigkeit abzustellen, reicht bei den Benachrichtigungspflichten jedoch nicht aus. Gerade Berufsgruppen, die auf den besonderen Schutz vertraulicher Kommunikation angewiesen sind, genießen in Zukunft ohnehin stärkere Abwehrrechte gegen Überwachung (Rn. 193). Entsprechend gewichtiger ist es, ihr Recht einzuschätzen, wenn sie trotz rechtlicher Hürden überwacht worden sind. Sie müssen in die Lage versetzt werden, den Rechtsweg zu beschreiten, um demokratisch hohe Güter wie etwa die Pressefreiheit oder das Vertrauensverhältnis zwischen Mandant- und Anwaltschaft verteidigen zu können. Wenn sie hingegen nur wissen, dass sie prinzipiell “attraktiv” als Ziel von Überwachungsmaßnahmen sind, aber nie

etwas davon erfahren, kann sich das Gefühl einer dauerhaften Überwachung einstellen, was sie in ihrer Grundrechtsausübung abschrecken kann.[23]

Benachrichtigungsfälle nach Staatsangehörigkeit und Grundrechtseingriff[24]				
		Staatsangehörigkeit		
		Deutsche oder in Deutschland befindliche ausländische Personen	EU- Bürger:innen	ausländische Personen im EU-Ausland
Grundrechtseingriff	Kernbereichsschutz durch Überwachung missachtet (Art. 1 GG)	zwingend	zwingend	zwingend
	Schutzbedürftigkeit bestimmter Berufsgruppen (z.B. Journalismus) durch Überwachung nicht gewahrt (z.B. Art. 5 GG)	zwingend	sehr hohes Interesse	hohes Interesse
	Telekommunikationsgeheimnis bei Überwachung eingeschränkt (Art. 10 GG)	zwingend	hohes Interesse	geringeres Interesse
	Menschenwürdegarantie durch Datenübermittlung ins Ausland missachtet (Art. 1 GG)	-	zwingend	zwingend

Dies gilt für Angehörige dieser Berufsgruppen universell und unabhängig von ihrer Nationalität. Wie Geheimdienste durch Digitalisierung und Internationalisierung ein gesteigertes Interesse an internationaler Kooperation haben, ist dies auch beispielsweise im Journalismus durch internationale Rechercheprojekte (Stichwort: Panama-Papers) oder im Strafrecht (Stichwort: unternehmerische Sorgfaltspflichten inländischer Firmen im Ausland) der Fall.

23 vgl. Assion, Simon (2014): Überwachung und Chilling Effects. In: Überwachung und Recht. Tagungsband zur Telemedicus Sommerkonferenz, S. 31-82, abrufbar unter: https://www.telemedicus.info/uploads/Dokumente/Ueberwachung-und-Recht-Tagungsband-Soko14.pdf sowie Staben, Julian (2016): Der Abschreckungseffekt auf die Grundrechtsausübung. Strukturen eines verfassungsrechtlichen Arguments. Tübingen, Mohr Siebeck.

24 Angenommen sind hier zwei Konstellationen: Einerseits wird die Kommunikation erst bei der menschlichen Filterung oder bei der menschlichen Auswertung als eine erkannt wird, die eigentlich nicht hätte überwacht werden dürfen, andererseits wird eine Überwachungsmaßnahme beendet, zum Beispiel weil sie nicht mehr erforderlich ist.

Diesen Trends würde der Grundrechtsschutz nicht gerecht, wenn bei internationalen Kooperationen ausländische Angehörige der Berufsgruppen von einer Überwachung nichts erfahren.

Eine Benachrichtigungspflicht ohne Ausnahme muss außerdem eingeführt werden, wenn sich bei ex post-Kontrollen herausstellt, dass Datenübermittlungen des BND ins Ausland zur Verletzung der Menschenwürde beigetragen haben, zum Beispiel weil Menschen im Zuge von Überwachungsmaßnahmen gefoltert wurden. Sie oder ihren Angehörigen muss es möglich sein, vor Gericht ihre Rechte einzuklagen, die Beteiligung deutscher Stellen an Menschenrechtsverletzungen rechtsstaatlich klären und gegebenenfalls Entschädigung einklagen zu können.

IV.1.8 Evaluationspflichten

Trotz der bereits genannten Berichtspflichten werden viele Schritte der Rechtskontrolle "Parlament und Öffentlichkeit weithin verschlossen bleiben" (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" (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".

Wer aber sollte dieser Evaluierungspflicht in der Praxis wie nachkommen? Hier sehen wir vor allem den Bundesdatenschutzbeauftragten und den Kontrollrat in der Pflicht, in regelmäßigen Abständen die Kontrolltätigkeiten kritisch auf ihre Wirksamkeit sowie auf Verbesserungs- und Anpassungsbedarf hin zu prüfen. Dafür empfiehlt sich auch der Austausch mit anderen europäischen Kontrollgremien, z.B. im Rahmen der European Intelligence Oversight Working Group, die ohne Beteiligung deutscher Aufsichtsbehörden bereits dabei ist, eine Plattform für neue effektivere Kontrollinstrumente und Methoden bereitzustellen.[25] Außerdem wäre auch hier die Expertise des neu zu schaffenden Beirats einzuholen.

Ein Beispiel für eine Evaluierungspflicht wäre die Datenlöschung. Um zu prüfen, ob der BND "Daten, die verfassungsrechtlich der inhaltlichen Sichtung entzogen sind, sofort ausgesondert sowie spurenlos und endgültig gelöscht" hat (Rn. 209), hat der BfDI die technischen Mittel der Filterung und Löschung weisungsunabhängig zu verifizieren. Sind sie wirklich geeignet, die Daten

25 siehe die Charter der European Intelligence Oversight Group, abrufbar unter: https://www.tet.dk/wp-content/uploads/2019/12/Charter-Intelligence-Oversight-Working-Group_signed-12-December-2019.pdf

spurenlos zu löschen oder werden diese Daten auf den Systemen lediglich überschrieben und somit nicht spurenfrei und unwiderruflich nach dem neuesten Stand der Technik entfernt? Diese Prüfung ist vielen datenbasierten Unternehmen und Behörden gemein, weshalb sich auf jeden Fall ein intensiver Austausch und die Einbindung des Beirats empfiehlt. Auch der strukturierte Austausch mit der Compliance-Abteilung des BND ist ratsam. Falls der BfDI diesbezüglich zum Ergebnis kommen sollte, dass die unabhängige Prüfung der Einhaltung von Löschpflichten nicht ausreichend gewährleistet sein kann, weil die vom BND zur Verfügung gestellten Protokolldaten diese Prüfung nicht zulassen, wäre vom Beanstandungsrecht Gebrauch zu machen und gegebenenfalls in Kontrolltechnologie zu investieren.

Ein weiteres Praxisbeispiel aus Dänemark verdeutlicht, was nötig sein kann, um die Wirksamkeit der Rechtskontrolle zu evaluieren. Dort hat die unabhängige dänische Aufsichtsbehörde TET einen systematischen Ansatz zur Risikoabschätzung entwickelt.[26] Insbesondere bei der administrativen Rechtskontrolle stellt sich schließlich wegen der vielen Prüfaufgaben die Frage, welche davon am dringlichsten sind. Die Mitarbeiter:innen des TET beantworten diese Frage, indem sie für bestimmte Nachrichtendienstsysteme Risikowerte berechnen, die ihnen helfen, Art und Zeitpunkt einer Kontrolltätigkeit zu bestimmen. Vor der Bestimmung eines Risikowertes für bestimmte nachrichtendienstliche Tätigkeiten – z.B. die Datenerfassung im Ausland durch informationstechnische Eingriffe in fremde Computer(-netzwerke) – bildet TET alle ihm bekannten Datenverarbeitungssysteme ab. Eine solche Übersicht der verschiedenen Speicherorte, Geräte, IT-Systeme und Software, mit denen die Dienste Daten sammeln, aufbewahren oder analysieren, ist entscheidend für eine aussagekräftige Risikobewertung.

Solche Aufgaben stellen an sich schon eine große Herausforderung dar. Darüber hinaus kann es sein, dass die Aufsichtsbehörde Teile der technischen Infrastruktur oder bestimmte Datenerhebungsmethoden des Bundesnachrichtendienstes überhaupt nicht kennen. Dementsprechend sollte die Identifizierung und Verfolgung bisher unbekannter Komponenten ein kontinuierlicher Teil der administrativen Rechtskontrolle sein. Das betrifft auch routinemäßige und spezifische Feedbackschleifen, die den Kontrolleur:inn helfen, die Wirksamkeit früherer Inspektionen und Untersuchungen systematisch zu bewerten. Zudem gilt es, das Modell der Risikobewertung ständig anzupassen und um neue Informationen zu ergänzen.

26 Kilian Vieth und Thorsten Wetzling führen in ihrem Papier “Datenbasierte Nachrichtendienstkontrolle” (siehe Literaturverzeichnis) weiterführende Informationen zur dänischen Praxis der Risikoabschätzung auf.

Neben der Evaluation der Kontrollpraxis fordern die Verfassungsrichter aber auch eine Evaluation der gesetzlichen Grundlagen. Das betrifft einerseits die gesetzlichen Vorgaben für die Kontrolle als auch die im Nachrichtendienst aufgeführten Dienstvorschriften und Schutznormen. Gerade mit Blick auf die ständige Evolution der Überwachungstechnik gilt es, regelmäßig den Rechtsrahmen kritisch zu prüfen und gegebenenfalls dem Gesetzgeber über Novellierungserfordernisse in Kenntnis zu setzen.

IV.2 Ressourcen der Rechtskontrolle

Neben den neu ins Nachrichtendienstrecht aufzunehmenden Vorgaben bedarf es dringender Investitionen, um bestehende Praktiken der Kontrolle zu stärken. Hier geht es einerseits um die Gewinnung von geeignetem Personal, dem deutlichen Ausbau von Zugriffsmöglichkeiten der Kontrolleur:innen auf Datenbanken und operationelle Systeme der Nachrichtendienste sowie die Nutzung und Fortentwicklung moderner, zum Teil automatisierter Kontrolltechnologie.

IV.2.1 Budget

Der Bundeshaushalt ist im Jahr 2018 gegenüber dem Jahr 2011 um 16 Prozent gestiegen, wohingegen sich die für den Bundesnachrichtendienst bewilligten jährlichen Haushaltsmittel in diesem Zeitraum verdoppelt haben (Rn. 107). Für das Jahr 2019 wurden 966,5 Millionen Euro für den BND bereitgestellt. Zusätzlich hat der Bund im Jahr 2018 rund 346 Millionen Euro für das Bundesamt für Verfassungsschutz und rund 96 Millionen Euro für den Militärischen Abschirmdienst bereitgestellt. Zusammen ergab dies im Jahr 2018 eine Milliarde und 438.5 Millionen Euro für die Nachrichtendienste auf Bundesebene.

Um nur ein Prozent dieser Ausgaben in die Kontrolle zu investieren, wären rund 14 Millionen Euro nötig. Gegenwärtig wird jedoch deutlich weniger darauf verwendet. Es ist mag müßig sein, die Kosten für Kontrolle exakt herunterzubrechen und Aufwände im Voraus exakt zu budgetieren. Als grobe Richtschnur hilft die Ein-Prozent-Forderung aber, um sich vor Augen zu halten, dass die Professionalisierung der Kontrolle zukünftig einen größeren Posten im Bundeshaushalt auskleiden sollte – zu offenkundig ist schließlich, dass die aktuellen Kontroll-Kapazitäten den gestiegenen Tätigkeiten der Nachrichtendienste nicht ansatzweise gewachsen sind.

Neben den bereits erhöhten Haushaltsgeldern für den BfDI und der parlamentarischen Kontrolle wäre in der Reform auch der unabhängige, gericht-

sähnliche Kontrollrat und – deutlich kleiner – der Beirat mit Bundesmitteln ausreichend auszustatten. Das heißt keineswegs, dass hinter allen Agent:innen ein:e Kontrolleur:in zu stehen hätte. Darum geht es nicht. Aber dem Gesetzgeber sollte eine wirksame Kontrolle künftig mehr Geld wert sein, wenn er am besonders umstrittenen Instrument der anlasslosen, breit angelegten Fernmeldeaufklrung festhalten will. Kontrolle schafft Vertrauen.

Das könnte zudem heißen, zukünftige Investitionen in die Nachrichtendienste stets nur mit weiteren Investitionen in die Kontrolle einzuführen. Schließlich bedarf es auch hier staatlicher Mittel, um beispielsweise Kontrollprogramme zu entwickeln (Rn. 288) und die Kontrollverfahren gegen digitale Angriffe zu sichern. Als minimale Vorgabe hat das Bundesverfassungsgericht vorgegeben, dass die Personalstärke der Rechtskontrolle nicht unter der Zahl an Mitarbeitenden in der Bundestagsverwaltung für die parlamentarische Kontrolle liegen darf (Rn. 288), was derzeit circa 35 bis 40 Personen wären.

IV.2.2 Zugang

Um die zahlreichen Befugnisse und -pflichten der administrative Rechtskontrolle in der Praxis wirksam und kontinuierlich auszuüben, hat der Gesetzgeber ihr einen “umfassenden Kontrollzugriff” (Rn. 272) zu ermöglichen. Dies gilt aber auch für den gerichtsähnlichen Spruchkörper. “Beiden Kontrollinstanzen ist umfassend Zugang zu allen Unterlagen einzuräumen. Dabei ist der BND dazu zu verpflichten, (...) Einsicht in Unterlagen und Daten, Aufschluss über verwendete Programme sowie jederzeitigen Zutritt zu Diensträumen zu gewähren” (Rn. 290). Das betrifft, wie oben beschrieben, auch den umfassenden Zugang zu Protokollen, die im Rahmen neuer Dokumentationspflichten anfallen.

Bezüglich des umfassenden Kontrollzugriffs hat Deutschland im westeuropäischen Vergleich noch deutlichen Aufholbedarf. Aufsichtsgremien wie IPCO (Großbritannien), CTIVD (Niederlande), CNCTR (Frankreich), AB-ND (Schweiz), TET (Dänemark), EOS (Norwegen) und SIUN (Schweden) sind hier besser aufgestellt. Wie Vieth und Wetzling im Rahmen von Fokusgruppentreffen mit Aufsichtsbehördern erfahren haben, können sich die Kontrolleur:innen in diesen Ländern bereits in die technischen Systeme der Nachrichtendienste einloggen und weisungsunabhängig Daten ihrer Wahl abrufen und auswerten. In einigen Ländern werden den Mitarbeitenden der Kontrolle spezielle Computerterminals in den Räumlichkeiten der Nachrichtendienste zur Verfügung gestellt.[27]

27 Diese Art des Zugangs vor Ort wird beispielsweise von den britischen, norwegischen und dänischen Aufsichtsbehörden genutzt.

So können die Kontrolleur:innen in Großbritannien die Nachrichtendienste beauftragen, bestimmte Daten zu extrahieren und in ein anderes System zu exportieren (z.B. im Format einer Kalkulationstabelle), um dann mit dieser Kopie weiterzuarbeiten.[28] Andere Aufsichtsbehörden können per Fernzugang von ihren eigenen Büros aus auf die technischen Systeme zugreifen.[29]Die Art des Zugriffs unterscheidet sich im internationalen Vergleich allerdings darin, ob die Kontrollorgane einen permanenten Zugang zu den nachrichtendienstlichen IT-Systemen und Datenbanken haben, oder ob sie von Fall zu Fall für einen begrenzten Zeitraum oder für eine bestimmte Untersuchung Zugang erhalten.

In der folgenden Tabelle haben wir aufgeführt, welche Zugänge auch in Deutschland in der anstehenden BND-Reform verankert werden sollten:

28 Auf diese Weise kann die Kontrollbehörde eine detaillierte Prüfung vornehmen, ohne die Systemintegrität des Dienstes zu beeinflussen.

29 Die schweizerische Unabhängige Aufsichtsbehörde verfügt über einen Fernzugriff auf Daten des Schweizer Nachrichtendienstes, was auch besonders geschützte personenbezogene Daten miteinschließt. Schweizer Nachrichtendienstgesetz (NDG), „Aufgaben, Informationsrechte und Empfehlungen der Aufsichtsbehörde", Art. 78 (5),“ 25. September 2015, https://www.admin.ch/opc/de/federal-gazette/2015/7211.pdf.

Art des Datenzugriffs	Beschreibung
Zugriff auf Quelldaten	Quelldaten sind „Rohdaten", die noch nicht für eine spätere Nutzung weiterverarbeitet wurden. Ihre Eigenschaften hängen von der jeweiligen Quelle der Daten ab, wie z.B. Fernmeldeaufklärung, offene Quellen, menschliche Quellen, Erwerb von Datensätzen von Unternehmen, Infiltration von Computernetzwerken, Satellitenaufklärung, etc. Bei der Fernmeldeaufklärung des BND sollte die Kontrolle ab dem Punkt möglich sein, wenn auch der BND die Daten in irgendeiner Weise verarbeitet, sei es zur automatisierten Filterung.
Zugriff auf Suchbegriffe (Selektoren)	Dies betrifft sowohl eigene als auch die von ausländischen Nachrichtendiensten übernommenen Suchbegriffe bei der Sichtung des erfassten Datenströme.
Zugriff auf Filtersysteme und dahinterliegende Schutzlisten	Automatisierte Systeme an verschiedenen Stufen des Filterprozesses arbeiten mit Datenbanken, die ihnen als "Filter-Referenz" dienen, zum Beispiel Telefonnummern besonders vor Überwachung zu schützender Personen. In Zukunft werden dies mindestens drei solcher Schutzlisten sein müssen, nämlich der Schutz von Deutschen, von Berufsgruppen mit besonderem Bedarf an Vertraulichkeit (z.B. Anwaltschaft, Journalismus) sowie der Kernbereichsschutz.
Zugriff auf gespeicherte Daten	Strukturierte Datenbanken, die z.B. Daten nach dem Filterprozess enthalten. Dies umfasst sowohl Verkehrs- als auch Inhaltsdaten.
Zugriff auf Protokolldaten	Verkehrsdaten über die Verwendung von Daten durch die Nachrichtendienste, beinhaltet u.a. die Auswahl, Sichtung, Übermittlung, Löschung und Auswertung von Daten.
Zugriff auf Auswertungen und Abkommen mit internationalen Partnern	Ein Einblick in die Ergebnisse der nachrichtendienstlichen Informationsgewinnung, die an die Bundesregierung übermittelt werden, bieten einen wichtigen Einblick in die Relevanz der zu genehmigenden Überwachungsmaßnahmen. Auch ist den Instanzen der Rechtskontrolle der Zugang zu Dokumenten zu gewähren, die strukturelle und ad hoc-Kooperationen mit ausländischen Nachrichtendiensten belegen.

Quelle: Vieth und Wetzling 2020, S.17.

Der direkte Zugang zu technischen Systemen birgt enormes Potenzial, denn er ermöglicht es den Aufsichtsbehörden, die Datenverarbeitung der Nachrichtendienste durch Stichproben, unangekündigte Inspektionen und (teil-) automatisierte Kontrollen zu überprüfen. Damit verringert sich die Abhängigkeit der Aufsichtsbehörden von (Einzel-)Informationen, die die Dienste selbst erst bereitstellen müssen. Der direkte Zugriff stellt einen zusätzlichen Anreiz dar, Datenschutzvorschriften durchweg umzusetzen und einzuhalten, weil die Beschäftigten der Nachrichtendienste nicht wissen können, ob ein bestimmter Vorgang überprüft wird.[30]

IV.2.3 Technologie

Erst ein verbesserter Zugang, beispielsweise zu den Protokolldaten, ermöglicht den erfolgreichen Einsatz moderner Kontrolltechnologie. Es ist daher wichtig, dass das Bundesverfassungsgericht erkannt hat, dass für eine wirksame Kontrolle der "Filterprozesse zur Aussonderung der Kommunikation von Deutschen und Inländern sowie zum Schutz von Vertraulichkeitsbeziehungen gegebenenfalls auch eigene Dateien und Kontrollprogramme zu entwickeln" sind (Rn. 288).

Um eine datenbasierte Nachrichtendienst-Kontrolle auch in Deutschland zu etablieren, sollten die Kontrollorgane ihre neu zu schaffenden Zugänge nutzen, um Mustererkennung zu betreiben. Beispielsweise können Prüfer:innen nach illegaler Datennutzung oder ungewöhnlichen Häufungen bestimmter Aktivitäten eine:r Analyst:in oder nach außergewöhnlich vielen Transaktionen in einer bestimmten Datei Ausschau zu halten. Die Prüfer:innen können auch potenzielle Probleme im Auge behalten, wie z. B. eine mehrfache Nutzung von Datenbanken von ungewöhnlichen Zugriffspunkten aus. Die Möglichkeiten zur Analyse von Logdateien reichen von einfachen deskriptiven Methoden (etwa der Vergleich von Durchschnitts-, Mittel-, Maximal- und Minimalwerten) bis hin zu komplexen Verfahren maschinellen Lernens oder statistischer Analysen. Datenanalyse-Software kann den Kontrolleur:innen helfen, die Nutzung von Datenbanken zu visualisieren sowie statistische Zusammenhänge und Netzwerke in den Protokolldaten zu erkennen und zu veranschaulichen.

Wenn die dem BfDI zur Verfügung gestellten Logdateien indes nur ganz rudimentär eine allgemeine Benutzung aufzeigen (z. B. „Datei wurde gelesen; Datei wurde gespeichert, Datei wurde geändert") schränkt das die Analysemöglichkeiten von Logdateien für Aufsichtszwecke erheblich ein. Von daher

30 weitere Informationen zu diesem Thema: Kilian Vieth und Thorsten Wetzling. 2020. Datenbasierte Nachrichtendienstkontrolle: Agenda für mehr Wirksamkeit. Berlin: Stiftung Neue Verantwortung.

sollte der vom Bundesverfassungsgericht geforderte umfassende Kontrollzugriff (Rn. 272) zukünftig weit auszulegen sein. Dies würde zudem der rechtlichen Anforderung gerecht, eine strikte Zweckeinhaltung zu gewährleisten (siehe Kapitel III.4).

Darüber hinaus wäre es denkbar, Warnmeldungen bei riskantem Datenaustausch einzuführen. Hier würden automatisierte Benachrichtigungen die Aufsichtsgremien über kennzeichnungspflichtige Datenweitergabe informieren, was auch gezielte Inspektionen im Nachgang ermöglichen würde. Besonders für die internationale Kooperation, in der der BND auch mit Staaten ohne funktionierenden Rechtsstaat Daten tauscht, ist dies wichtig.

Eine Analyse der Datenverarbeitung beim BND ist auch für die praktische Nachverfolgung der Umsetzung genehmigter Überwachungsanordnungen bedeutsam. Mittels digitaler Prüfpfade (audit trails) könnte beispielsweise die konkrete Umsetzungen von genehmigten Ausleitungen bei Netzbetreibern und der Weg, den die Daten aus dieser Maßnahme im Verlauf der Datenverarbeitung nehmen, dokumentiert und über einen längeren Verlauf verfolgt und verglichen werden. Dies ermöglicht es der Rechtskontrolle, die Notwendigkeit neuer Anordnungen im Lichte der abgeschlossenen und bereits laufenden Überwachungsmaßnahmen besser zu beurteilen. Zudem kann es dem Spruchkörper helfen, unzureichend begründete Anträge bzw. unzulässige Wiederholungen in den Antragsbegründungen aufzuspüren, weil Vergleichsdaten aus der Vergangenheit vorliegen.[31]

31 Auch diese Ideen entstammen dem von Kilian Vieth und Thorsten Wetzling verfassten Papier zur “datenbasierten Nachrichtendienstkontrolle” (siehe Literaturverzeichnis).

V. Weitere Herausforderungen für Nachrichtendienstrecht und Kontrollpraxis

In ihrem Grundsatzurteil legen die Verfassungsrichter:innen detailliert dar, wo in der Ausland-Ausland-Fernmeldeaufklärung einschneidende Reformen des Gesetzes und der Praxis nötig sind. Dies müsste die Bundesregierung und den Bundestag ausgiebig beschäftigen. Dabei sollte der Gesetzgeber die Gelegenheit nicht verstreichen lassen, auch bei weiteren, seit längerem bekannten, Baustellen der Nachrichtendienst-Politik tätig zu werden. Im Folgenden werden wir einige davon skizzieren, nämlich ein möglicher Einsatz des Bundestrojaners durch den BND (V.1), die Reform des Bundesamts für Verfassungsschutz (V.2) sowie die Auslandsaufklärung durch und für die Bundeswehr (V.3).

V.1 Einsatz des Bundestrojaners durch den BND

Anders als andere europäische Gesetzgeber hat der Bundestag bis dato für weitere *bulk powers*, wie gebündelte informationstechnische Eingriffe in fremde Computer(-netzwerke) oder das massenhafte Abgreifen und Verarbeiten von Datenbanken aus dem Privatsektor, keine gesetzliche Grundlage geschaffen, wie sie nach Art. 10 Abs. 2 GG notwendig wäre. Der BND ist also derzeit nicht ermächtigt, Hacking-Tools wie den sogenannten Bundestrojaner einzusetzen, um verschlüsselte Kommunikation mitzulesen (sog. Quellen-TKÜ) oder gar fremde Geräte remote zu durchsuchen (sog. Online-Durchsuchung) – weder im Einzelfall, noch massenhaft. Aus einem geleakten Gesetzesentwurf des Bundesinnenministeriums ist jedoch bekannt, dass die Bundesregierung im Grundsatz auch hier gesetzliche Grundlagen schaffen wollte.[32]

Nach dem Karlsruher Grundsatzurteil ist klargestellt, dass der Einsatz solcher Hacking-Tools zur Überwachung von Kommunikation wie auch im Inland (mindestens) an Artikel 10 GG und am sogenannten “Computer-Grundrecht” zu messen sein wird – egal wo auf der Welt der BND sie einsetzen möchte, sei es bei gezielten Überwachungen oder gar im Sinne eines “bulk hacking”. Der alleinige Verweis auf § 1 Abs. 2 BND-Gesetz wird nicht (mehr) genügen.

32 siehe: Andre Meister und Anna Biselli. 2019. Wir veröffentlichen den Gesetzentwurf: Seehofer will Staatstrojaner für den Verfassungsschutz. Netzpolitik.org , 28.03.2019, abrufbar unter: https://netzpolitik.org/2019/wir-veroeffentlichen-den-gesetzentwurf-seehofer-will-staatstrojaner-fuer-den-verfassungsschutz/

Beim Bundestrojaner muss der Staat aktiv Sicherheitslücken in Soft- und Hardware offen halten, um Personen überhaupt hacken zu können. Es stellt sich daher vor allem die politische Frage, ob man Nachrichtendiensten diese Mittel überhaupt an die Hand geben möchte. Wir haben erhebliche Zweifel, da ein Offenhalten von Sicherheitslücken immer auch eine Gefahr für die gesamte Bevölkerung darstellt, weil auch kriminelle Gruppen oder ausländische Nachrichtendienste sie ausnutzen können. Dies gilt schon bei gezielten Überwachungsmaßnahmen, erst recht aber beim "bulk hacking", in der gewissermaßen wahllos Geräte gehackt werden, um daraus Informationen "abzusaugen". Es ist eben nicht wie strategische Fernmeldeaufklärung "nur" ein passives Mitlesen, sondern ein aktiver Angriff auf die IT-Geräte von Personen.

Sofern es einen politischen Willen dazu geben sollte, müsste diese Diskussion zumindest zunächst im Rahmen einer Verbändeanhörung und anschließender Erörterung im Bundestag geführt werden. Eine gesetzliche Grundlage kann nicht – wie im 2019 geleakten BMI-Entwurf – *en passant* in das BND-Gesetz übernommen werden.

V.2 Reform des Verfassungsschutzrechts

Eine umfassende Analyse des im April 2019 auf netzpolitik.org veröffentlichten "Gesetzentwurf zur Harmonisierung des Verfassungschutzrechts"[33] steht nicht im Fokus dieses Papiers. Es wäre aufgrund der an Fahrt gewonnen Ressortabstimmung zum Verfassungsschutz-Gesetz wohl auch nicht mehr zeitgemäß. Medienberichten zufolge scheinen in den interministriellen Beratungen einige kritikwürdige Passagen im zweiten Referententwurf herausgenommen worden zu sein.[34]

Dennoch sei für diese Diskussion an die Klarstellung der Verfassungsrichter:innen erinnert, dass "dem Bundesnachrichtendienst (...) nur Aufgaben und Befugnisse übertragen werden, die eine außen- und sicherheitspolitische Bedeutung haben und damit eine internationale Dimension aufweisen" (Rn. 127). Daher sind in einer zukünftigen Novellierung des Verfassungsschutzrechts beispielsweise lokale Amtshilfen des BND bei der Wohnraumüberwachung, der Quellen-TKÜ oder sogar der Online-Durchsuchung auszuschließen.

33 siehe Meister, Andre, Biselli, Anna. 2019.

34 Meister, Andre. 2020. Bundesregierung einigt sich auf Staatstrojaner für Inlandsgeheimdienst. 04.06.2020, abrufbar unter: https://netzpolitik.org/2020/bundesregierung-einigt-sich-auf-staatstrojaner-fuer-inlandsgeheimdienst/

Unabhängig von der Frage, welche rechtlichen Überwachungsbefugnisse dem Inlandsgeheimdienst bei der Reform zu- oder abgesprochen werden, muss die Ausgestaltung der Rechtskontrolle des BfV auch am Karlsruher Grundsatzurteil zur Ausland-Ausland-Fernmeldeaufklärung zu messen sein – und nicht mehr (nur) am Artikel 10-Gesetz. Sowohl das Artikel 10-Gesetz als auch die institutionelle Aufstellung samt Kontrollrechte der G10-Kommission ist nicht mehr zeitgemäß. Die G10-Kommission operiert nach Aussagen einiger Mitglieder schon heute am Limit ihrer Kapazitäten und würde mit den im Raum stehenden Befugniserweiterungen im Verfassungsschutzrecht weitere Kontrollaufgaben erhalten. Die heutige Praxis scheint mit den verfassungsrechtlichen Anforderungen kaum vereinbar, wenn etwa "eine vom BMI angeordnete Beschränkungsmaßnahme mehrere Wochen durchgeführt wird, ohne dass die G10-Kommission mit dieser befasst war"[35]. Da diese Praxis "angesichts der klaren Aussagen des EGMR in seinem – die ungarische Rechtslage betreffenden – Urteil vom 12. 1. 2016 als konventionswidrig erweisen" könnte, muss der Turnus der Sitzungen schon bis zur "Karlsruher Deadline" Ende 2021 dringend erhöht werden. Auch sollte die Bundesregierung bis Ende 2021 nicht mehr auf ehrenamtliche Mitglieder in der Rechtskontrolle des Verfassungsschutzes zurückgreifen.

Perspektivisch braucht es jedoch moderne, und wir glauben: neue Strukturen der Kontrolle aller Nachrichtendienste, die in einer Institution gebündelt werden sollten. Die Fragmentierung der Kontrollinstitutionen muss ein Ende haben, indem Kontrollrat und BfDI die alleinige Befugnis für die Rechtskontrolle übertragen würde – nicht nur für den BND, sondern auch für BfV und MAD.

V.3 Auslandsaufklärung der Bundeswehr

Die Bundeswehr war nicht Gegenstand des Verfahrens, welches nun zum Grundsatzurteil zur Ausland-Ausland-Fernmeldeaufklärung führte. Da überrascht es nicht, dass sich das Bundesverfassungsgericht ein obiter dictum im Urteil verkniffen hat und etwa auch zu Beginn der mündlichen Verhandlung klarstellte, dass es bei der Frage der extraterritorialen Gültigkeit des Art. 10 GG nicht etwa auch um Fragen zu zu Auslandseinsätzen der Bundeswehr gehe. Dennoch ist das Urteil nicht völlig unbedeutend für die Arbeit der Bundeswehr.

35 Huber, Bertold. 2017. "Kontrolle der Nachrichtendienste des Bundes - dargestellt am Beispiel der Tätigkeit der G 10-Kommission", Zeitschrift für das Gesamte Sicherheitsrecht, 01/2017, S. 15-16.

Die Bundeswehr verfügt 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).[36]

Inwiefern diese einzelnen Maßnahmen Eingriffe in das Grundrecht aus Art. 10 GG darstellen und inwiefern für sie daher im Lichte des Karlsruher Urteils auch eine unabhängige objektivrechtliche Rechtskontrolle vonnöten ist, kann hier nicht abschließend erörtert werden. Zumindest aber scheint das Argument, wonach im Rahmen der militärischen Aufklärung "Informationen lediglich über (potentielle) gegnerische Kräfte gesammelt werden, die grundsätzlich ohnehin nicht grundrechtsfähig seien" und daher "keine Ermächtigungsgrundlage im Bundesrecht erforderlich" sei, so nicht mehr haltbar zu sein.[37]

Ganz grundsätzlich sollte ohnehin überlegt werden, ob die militärische Aufklärung und die elektronische Kampfführung der Bundeswehr nicht als nachrichtendienstliche Tätigkeiten des Bundes einer wirksameren Kontrolle unterliegen sollten. Zur Vermeidung von Kontrolllücken wäre es sowohl für die parlamentarische Kontrolle als auch für die Rechtskontrolle wünschenswert, sie auf alle "nachrichtendienstlichen Tätigkeiten des Bundes" (Art. 45d GG) auszuweiten, anstatt allein auf die "Tätigkeit(en) des Bundesamtes für Verfassungsschutz, des Militärischen Abschirmdienstes und des Bundesnachrichtendienstes" (§1 Abs. 1 PKGr-Gesetz) abzustellen. Ein internationales Beispiel hierfür wären die Reformen in Großbritannien oder Kanada. Dort wird bei der Kontrolle fortan nach Tätigkeiten und nicht nach Behörden

36 Diese Informationen wurden diesen Quellen entnommen: https://de.wikipedia.org/wiki/Nachrichtengewinnung_und_Aufkl%C3%A4rung; https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-strategische-aufklaerung; https://de.wikipedia.org/wiki/Elektronische_Kampff%C3%BChrung

37 Mareike Neumann, 2020. 3. Symposium zum Recht der Nachrichtendienste – Nachrichtendienste in vernetzter Sicherheitsarchitektur, Kriminalpolitische Zeitschrift 3/2020. https://kripoz.de/2020/01/24/3-symposium-zum-recht-der-nachrichtendienste-nachrichtendienste-in-vernetzter-sicherheitsarchitektur/

unterschieden. Zum Beispiel unterliegen alle kanadischen Sicherheitsbehörden, die nachrichtendienstliche Tätigkeiten betreiben, der gleichen Kontrolldichte durch die gleiche Kontrollinstanz (NSIRA).[38] Damit kann verhindert werden, dass die Exekutive nachrichtendienstliche Tätigkeiten von einer Behörde zur anderen delegiert, um so einer strengeren Kontrolle auszuweichen.

38 Siehe "Ganzheitliche und behördenübergreifende Prüfung von SIGINT-Aktivitäten" in Wetzling und Vieth 2019, S. 83.

VI. Fazit

Ein Großteil der Geheimdienstreform von 2016 ist verfassungswidrig. Die Liste der gesetzlichen Schranken und Kontrollvorgaben, die der Bundestag nun bis Ende 2021 ins Nachrichtendienstrecht aufzunehmen hat, ist entsprechend lang. Das Urteil des Bundesverfassungsgerichts zum BND-Gesetz sollte den Verantwortlichen in Bundestag und Bundesregierung klarmachen, dass es im zweiten Anlauf deutlich höherer Anforderungen bedarf, um die Überwachungsbefugnisse der Nachrichtendienste rechtsstaatlich einzuhegen und sie wirksamer zu kontrollieren.

Im Vorfeld eines für die nächsten Wochen angekündigten Eckpunktepapiers des Bundeskanzleramts, und dann wohl zügigen Gesetzgebungsprozesses, zeigt dieses Papier konkrete Möglichkeiten auf, wie der Gesetzgeber die weitreichenden Forderungen der Karlsruher Verfassungsrichter:innen zur Praxis der strategischen Fernmeldeaufklärung und ihrer Kontrolle umsetzen könnte. Wir sehen in der BND-Reform 2.0 eine Chance, die fragmentierte und untertourig laufende Kontrolllandschaft in Deutschland zu entrümpeln und dadurch zu stärken. Zudem könnte der Gesetzgeber das durch mehrgliedrige Verweisungsketten unnötig komplexe Nachrichtendienstrecht jetzt so vereinfachen, dass am Ende eine klare Rechtsgrundlage mit internationaler Vorbildfunktion entsteht.

Dafür braucht es einen Kraftakt und den nötigen Reformwillen. Das vom Kanzleramt vorgegebene Tempo lässt nicht darauf schließen. Wer wirklich nur das juristisch zwingend notwendige im BND-Gesetz verändert will, verkennt die weitreichenden Konsequenzen, die eine gründliche Analyse des Grundsatzurteils ergeben hat. Konkret: Wer jetzt nicht auch im Artikel 10- und PKGr-Gesetz für wesentliche Verbesserungen sorgt, der nimmt die unnötige Fragmentierung der “gerichtsähnlichen Spruchkörper” weiter in Kauf und ändert nichts an dem völlig unzureichenden Status Quo der “administrativen Rechtskontrolle” für Maßnahmen der Inland-Ausland-Aufklärung. Die unzureichende grundrechtliche und datenschutzrechtliche Kontrolle darf außerdem nicht mehr durch eine Aufstockung der parlamentarischen Kontrolle kaschiert werden.

Ohne echte Reform würde das zwingend nötige Vertrauen der Bevölkerung in die Arbeit des BND weiter Schaden nehmen, zumal dies nach der verfassungsrechtlichen Quittung ohnehin gelitten hat. Wer die strategische Fernmeldeaufklärung im Zeichen der Sicherheit will, kommt um eine entsprechende Stärkung von balancierenden Freiheits- und Kontrollrechten in

Zukunft nicht mehr herum. Eine unabhängige Kontrolle sollte daher weniger abhängig von den Unterrichtungen der Bundesregierung sein, sondern diese durch einen umfassenden Kontrollzugriff (Rn. 272) eigenständig gewährleisten.

VII. Literatur- und Internetquellen

Assion, Simon. 2014. “Überwachung und Chilling Effects”, in: Überwachung und Recht. Tagungsband zur Telemedicus Sommerkonferenz, S. 31-82, abrufbar unter: https://www.telemedicus.info/uploads/Dokumente/Ueberwachung-und-Recht-Tagungsband-Soko14.pdf

Bradford Franklin, Sharon. 2020. “A Key Part of Surveillance Reform Is now in Jeopardy”. 29. Mai 2020, abrufbar unter: https://slate.com/technology/2020/05/usa-freedom-reauthorization-act-fisa-reform-surveillance-amicus-curiae.html

Deutscher Bundestag. 2013. “Beschlussempfehlung und Bericht des NSU-Untersuchungsausschusses”. Drucksache 17/1460022, abrufbar unter: https://dipbt.bundestag.de/dip21/btd/17/146/1714600.pdf

Diehl, Jörg, Lehberger, Roman, Schmid, Fidelius. 2020. Undercover. Ein V-Mann packt aus. DVA: München.

Esposito, Elena 2007. Die Fiktion der wahrscheinlichen Realität. Frankfurt am Main: Suhrkamp.

European Intelligence Oversight Group. Charter, abrufbar unter: https://www.tet.dk/wp-content/uploads/2019/12/Charter-Intelligence-Oversight-Working-Group_signed-12-December-2019.pdf

Investigatory Powers Commissioner’s Office (IPCO). 2020. Annual Report 2018, abrufbar unter: https://ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf

Hipp, Dietmar, Hoppenstedt, Max, Knobbe, Martin und Wiedemann-Schmidt, Wolf. 2020. “BND kann bis zu 1,2 Billionen Verbindungen pro Tag abzweigen, abrufbar unter: https://www.spiegel.de/netzwelt/netzpolitik/bnd-kann-bis-zu-1-2-billionen-verbindungen-pro-tag-abzweigen

Huber, Bertold. 2017. “Kontrolle der Nachrichtendienste des Bundes - dargestellt am Beispiel der Tätigkeit der G 10-Kommission”, Zeitschrift für das gesamte Sicherheitsrecht, 12-16.

Knobloch, Tobias. 2018. Vor die Lage kommen: Predictive Policing in Deutschland. Stiftung Neue Verantwortung: Berlin, abrufbar unter: https://www.stiftung-nv.de/de/publikation/vor-die-lage-kommen-predictive-policing-deutschland

Meister, Andre und Biselli, Anna. 2019. “Wir veröffentlichen den Gesetzentwurf: Seehofer will Staatstrojaner für den Verfassungsschutz”, 29. März 2019, abrufbar unter:

https://netzpolitik.org/2019/wir-veroeffentlichen-den-gesetzentwurf-seehofer-will-staatstrojaner-fuer-den-verfassungsschutz/

Meyer-Fünffinger, Arne, Tanriverdi, Hakan und Zierer, Maximilian. 2020. "So überwacht der BND das Internet. Auslandsgeheimdienst". Tagesschau. de. 15. Mai 2020, abrufbar unter: https://www.tagesschau.de/investigativ/br-recherche/bnd-urteil-101.html

Moßbrucker, Daniel. 2020. "Urteil zum BND-Gesetz. Quellenschutz im Zeitalter digitaler Massenüberwachung". Netzpolitik.org. 25. Mai 2020, abrufbar unter: https://netzpolitik.org/2020/was-heisst-quellenschutz-im-zeitalter-digitaler-massenueberwachung/

Redaktionsnetzwerk Deutschland. 2020. "Braun will BND schnell Sicherheit verschaffen". n-tv.de. 03. Juni 2020, abrufbar unter: https://www.n-tv.de/politik/Braun-will-BND-schnell-Sicherheit-verschaffen-article21821641.html

Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung. o.D. "Funkzellenabfragen-Transparenz-System". fts-berlin.de, abrufbar unter: https://fts.berlin.de/

Staben, Julian. 2016. Der Abschreckungseffekt auf die Grundrechtsausübung. Strukturen eines verfassungsrechtlichen Arguments. Tübingen: Mohr Siebeck Verlag.

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS). 2019. "Annual Report 2018", abrufbar unter: https://eos-utvalget.no/wp-content/uploads/2019/05/eos_annual_report_2018.pdf

Technological Advisory Panel. 2019. "TAP Working Protocol", abrufbar unter: https://www.ipco.org.uk/docs/TAP%20working%20protocol%20(25%20March%202019)%20FINAL.pdf

Toetsingscommissie Inzet bevoegdheden (TIB). 2020. Annual report 2018/2019, abrufbar unter: https://www.tib-ivd.nl/binaries/tib/documenten/jaarverslagen/2019/04/25/annual-report-2018-2019/TIB+Annual+Report+2018-2019.pdf

Vieth, Kilian und Wetzling, Thorsten. 2020. "Datenbasierte Nachrichtendienst-Kontrolle: Agenda für mehr Wirksamkeit". Stiftung Neue Verantwortung: Berlin, abrufbar unter: https://www.stiftung-nv.de/en/node/2823

Wetzling, Thorsten und Kilian Vieth. 2019. "Massenüberwachung bändigen: Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich". Heinrich Böll Stiftung: Berlin, abrufbar unter: https://www.boell.de/sites/default/files/massenueberwachung-baendigen_kommentierbar.pdf

United Nations. 2014. Resolution 68/167 zum Recht auf Privatheit im digitalen Zeitalte, abrufbar unter:. https://undocs.org/A/RES/68/167

Danksagung

Die Autoren bedanken sich herzlich für die sachkundige und tatkräftige Unterstützung von Kilian Vieth, Charlotte Dietrich und Gina Butros bei der Erstellung dieser Studie. Desweiteren gilt unser Dank den Mitarbeiter:innen und Mitgliedern der G10-Kommission, des BfDI sowie der Bundestagsfraktionen im Bundestag, mit denen wir im Nachgang der Urteilsverkündung zum BND-Gesetz im Austausch standen. Für den Inhalt dieser Studie sind die Autoren allein verantwortlich.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über die Autoren

Thorsten Wetzling leitet die Arbeit der Stiftung Neue Verantwortung im Themenfeld Grundrechte, Überwachung und Demokratie. Er führt das Europäische Netzwerk Nachrichtendienst-Kontrolle (EION) und ist Principal Investigator im Verbundprojekt guardint.org, das von der DFG finanziert wird. Zudem ist Thorsten Editor in Chief des englischsprachigen Blogs aboutintel.eu. Er hat am Genfer Hochschulinstitut für internationale Studien und Entwicklung mit einer vergleichenden Studie zur Performanz und Reform der Nachrichtendienst-Kontrolle in Europa promoviert.

Daniel Moßbrucker, M.A., promoviert am Fachgebiet Journalistik und Kommunikationswissenschaft der Universität Hamburg zum Thema “Journalismus und Überwachung”. Er arbeitet in Berlin als Journalist zu den Themen Überwachung, Datenschutz und Internetregulierung und trainiert außerdem Journalist:innen im In- und Ausland in digitaler Sicherheit. Von 2016 bis 2019 war er hauptamtlicher Referent für Internetfreiheit bei Reporter ohne Grenzen und in diesem Zusammenhang beteiligt an der Verfassungsbeschwerde der Organisation gegen das BND-Gesetz.

So erreichen Sie die Autoren

Dr. Thorsten Wetzling
twetzling@stiftung-nv.de
+49 (0)30 81 45 03 78 80
@twetzling

Daniel Moßbrucker
mail@daniel-mossbrucker.de
(PGP: 9C4E D204)
@damossb

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Grafiken:
Anne-Sophie Stelke