STELLUNGNAHME VON AMNESTY INTERNATIONAL ZUM ENTWURF EINES GESETZES ZUR ÄNDERUNG DES BND-GESETZES, DRUCKSACHE 19/26103

Berlin, 17.02.2021

A. VORWORT

Die Bundesregierung hat mit der anstehenden Neufassung des BND-Gesetzes die Gelegenheit, mit einem **gesetzgeberischen "Neustart"** die Überwachungsbefugnisse des BND sowie seine Kontrolle neu zu fassen. Es gilt die von Überwachungsvorgängen betroffenen Menschenrechte angemessen zu schützen und dabei auch international mit gutem Beispiel voranzugehen. Dem vorliegenden Entwurf gelingt dies an vielen Stellen noch nicht, auch die Maßgaben des Bundesverfassungsgerichts werden nicht vollständig umsetzt. Diese Maßgaben tragen auch dazu bei, dass Deutschland seine **völkerrechtliche Verpflichtung zur Achtung der Menschenrechte** in diesem sensiblen Bereich staatlichen Handelns erfüllen kann. In diesem Sinne stellen die nachfolgend kritisierten **Defizite der Umsetzung des Urteils Indizien für eine Verletzung menschenrechtlicher Pflichten Deutschlands** dar (insbesondere des Rechts auf Privatleben, wie es sich etwa aus Art. 8 EMRK, Art. 12 IPbpR ergibt), die beseitigt werden müssen.

Es sei darauf hingewiesen, dass die **Frage der menschenrechtlichen Vereinbarkeit anlassloser Massenüberwachung für Zwecke der nationalen Sicherheit** derzeit auch Gegenstand eines laufenden Verfahrens vor dem EGMR ist.[1] Die nachfolgende Kommentierung orientiert sich im Wesentlichen an der bereits erfolgten Rechtsprechung des BVerfG, auf deren Grundlage die Änderung des BND-Gesetzes erfolgen muss.

Der Gesetzentwurf **schränkt die bestehenden Überwachungsbefugnisse des BND kaum ein und erweitert sie an einigen Stellen sogar** (etwa bei der erweiterten „Eignungsprüfung“ und dem Einsatz von Hacking für die Überwachung verschlüsselter Kommunikation). Die vom Bundesverfassungsgericht geforderte sogenannte **"Überwachungsgesamtrechnung"** hat die Bundesregierung noch immer nicht erstellt. Sie wäre nach Ansicht von Amnesty International eine notwendige Grundlage für Entscheidungen über weitere gesetzgeberische Eingriffe in das Menschenrecht auf Privatsphäre.

Aus zeitlichen Gründen nimmt Amnesty International nur zu ausgewählten Regelungen des vorliegenden Gesetzentwurfs Stellung. Dies bedeutet nicht, dass die Organisation bezüglich aller anderen Regelungen keine menschenrechtlichen Bedenken hat.

B. ZUSAMMENFASSUNG DER SCHWERWIEGENDSTEN DEFIZITE UND VORSCHLÄGE ZUR ABHILFE

[1] 10 Human Rights Organisations and others v. United Kingdom (no. 24960/15), siehe auch Amnesty-Stellungnahme für den EGMR, Online: https://www.amnesty.org/en/documents/eur45/0646/2019/en/

AMNESTY INTERNATIONAL Sektion der Bundesrepublik Deutschland e. V.
Politik und Activism . Zinnowitzer Straße 8 . 10115 Berlin
T: +49 30 420248-0 . F: +49 30 420248-444 . E: lena.rohrbach@amnesty.de . W: www.amnesty.de

SPENDENKONTO . Bank für Sozialwirtschaft
IBAN: DE 233 702050 0000 8090100 . BIC: BFS WDE 33XXX

AMNESTY INTERNATIONAL

(Begründungen sowie weitere Punkte werden im folgenden Volltext ausgeführt)

- **Ungenügende Beschränkungen der strategischen Aufklärung:**
  - Die Voraussetzungen für die Zulässigkeit einer strategischen Aufklärungsmaßnahme gemäß § 19 BNDG-E sind - auch gegenüber dem Urteil des BVerfG - zu weit gefasst. Nachschärfungen sind erforderlich, insbesondere hinsichtlich der genannten Gefahrenbereiche.
  - Das zulässige Datenvolumen ist mit 30 Prozent der Telekommunikationsnetze nicht wirksam beschränkt, da die Anzahl der überwachten Netze nichts über das überwachte Datenvolumen aussagt. Die Begrenzung sollte stattdessen anhand der Datenmenge definiert und um eine Begrenzung des abgedeckten geographischen Gebiets ergänzt werden.

- **Ungenügende Verwendungsbeschränkung:** Die Differenzierung zwischen den Aufklärungszwecken (§ 19 Abs. 10 BNDG-E) ist zu grob, stattdessen sollte nach den unter § 19 Abs. 4 benannten konkreten Aufklärungszwecken differenziert werden.

- **Die geplante „Eignungsprüfung" stellt ein Einfallstor für unkontrollierte, anlasslose Massenüberwachung dar.** Die Anordnung kann immer wieder verlängert werden und die Möglichkeiten für eine Weiterverarbeitung und langfristige Speicherung der erhobenen Daten wurden ausgeweitet. Nicht nachvollziehbar ist, warum die Anordnungen und Weiterverarbeitungsbefugnisse nicht der Kontrolle durch den Unabhängigen Kontrollrat unterliegen. Zusätzlich unterliegen Eignungsprüfungen nicht der Beschränkung auf 30 Prozent der Telekommunikationsnetze. Die Möglichkeit einer Eignungsprüfung muss gestrichen oder wenigstens in Überwachungsvolumen und Dauer deutlich begrenzt sowie der Kontrolle unterworfen werden.

- **Die Regelungen für Datenübermittlungen** an inländische (§ 29) sowie ausländische (§ 30) Stellen geben Anlass zu einer Reihe von Bedenken bzgl. zu niedrig angesetzter Übermittlungsschwellen, möglicher Automatisierung, fehlender Begrenzungen und Beschränkungen und Zweifeln an der Normenklarheit und Verhältnismäßigkeit (siehe Volltext). Zusätzlich genügt die Regelung in § 30 Abs. 6 BNDG-E, aus der sich ergibt, in welchen Fällen Daten nicht an ausländische Stellen weitergegeben werden dürfen, nicht den Anforderungen des BVerfG. Sie kann Betroffene auch nicht hinreichend vor weiteren Menschenrechtsverletzungen in Folge der Weitergabe sie betreffender Daten an eine ausländische Stelle schützen.

- **Eingriffe in informationstechnische Systeme (Hacking)** sind nach Ansicht von Amnesty unverhältnismäßig im Bereich der politischen Unterrichtung der Bundesregierung (§ 34 Abs. 1 Satz 1 Nr. 1 BNDG-E), auch bei der Gefahren-Früherkennung erscheint die Verhältnismäßigkeit nur schwer vorstellbar. Sofern dennoch an dieser Befugniserweiterung für den BND festgehalten werden soll, müssen dringend zusätzliche Maßnahmen bzgl. der Anordnungen, Minimierung von Manipulationsrisiken und Protokollierung eingeführt werden. Zusätzlich muss ein Schwachstellenmanagement vorgesehen werden, also ein Prozesses, der die Verhältnismäßigkeit der Ausnutzung einer Schwachstelle prüft und dabei die damit verbundenen Risiken einer fortdauernden Geheimhaltung für die Allgemeinheit angemessen berücksichtigt. Amnesty setzt sich für zahlreiche Menschrechtsverteidiger_innen weltweit ein,

deren Kommunikation unter Ausnutzung nicht bekannter Sicherheitslücken überwacht wurde und wird.[2]

- **Die Perspektive der von Überwachung Betroffenen sollte im unabhängigen Kontrollrat dringend gestärkt werden.** Dafür sollte ein kontradiktorisches Verfahren eingeführt werden (auch, um die vom BVerfG geforderte "Gerichtsähnlichkeit" zu erreichen), möglichst durch explizite Aufnahme eines "Anwalts/Anwältin der Menschenrechte". Zudem ist die Einrichtung eines Expert_innenbeirats empfehlenswert.

- **Die Kontrolle durch den Kontrollrat ist lückenhaft:**
  - Dem gerichtsähnlichen Kontrollorgan sollten auch die Suchmerkmale (Selektoren) zur Prüfung vorgelegt werden.
  - Die Prüfkompetenzen des Kontrollrates sollten auf Verkehrsdaten und sogenannte "Sachdaten ohne Personenbezug" ausgeweitet werden.
  - Unbedingt müssen die sogenannten "Eignungsprüfungen" nach §24 einer Kontrolle durch beide Organe des Unabhängigen Kontrollrates unterworfen werden.
  - Im Bereich der internationalen Kooperationen besteht Präzisierungsbedarf bei der Kontrolle (siehe Volltext).

- **Der Weg zu einer Beanstandung durch den Kontrollrat dauert zu lange**, er sollte vereinfacht und verkürzt werden, zudem es bedarf es der Aufnahme explizierter Sanktionsmöglichkeiten für den Kontrollrat und einer Stärkung der Kontrolle durch den BfDI durch die Möglichkeit von Anordnungen.

B. AUSFÜHRLICHE BETRACHTUNG DES GESETZENTWURFES

ZUR STRATEGISCHEN AUSLAND-FERNMELDEAUFKLÄRUNG, § 19 BNDG-E:

- **Die Voraussetzungen für die Zulässigkeit einer strategischen Aufklärungsmaßnahme** gemäß § 19 BNDG-E sind gegenüber den klaren Maßgaben des BVerfG noch **zu weit gefasst.** So bleibt die Formulierung hinsichtlich der Gefahrenfrüherkennung (§ 19 Abs. 1 Nr. 2, Abs. 4 BNDG-E) deutlich hinter den Vorgaben des BVerfG zurück. Danach müsse die Aufklärungstätigkeit auf den Schutz hochrangiger Gemeinschaftsgüter gerichtet sein, deren Verletzung schwere Schäden für den äußeren und inneren Frieden oder die Rechtsgüter Einzelner zur Folge hätte (BVerfG, Rn. 176). Die derzeit vorgesehene Regelung spiegelt diese hohen Anforderungen noch nicht ausreichend wider, sondern verlangt lediglich, dass die Informationen „von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland“ sind und tatsächliche Anhaltspunkte für die Möglichkeit vorliegen, Erkenntnisse zu bestimmten, benannten Gefahrenbereichen oder zum Schutz bestimmter benannter Rechtsgüter zu gewinnen. Insbesondere bei den benannten **Gefahrenbereichen sind Nachschärfungen** zwingend erforderlich, um die Maßgaben des BVerfG angemessen umzusetzen. Besonders deutlich wird dies an den Formulierungen in § 19 Abs. 4 Nr. 1 lit. b (krisenhafte Entwicklungen im Ausland

[2] Siehe Amnesty International, Bericht „Gezielte Überwachung von Menschenrechtsverteidigern“, 2020, online: https://www.amnesty.de/sites/default/files/2020-09/Amnesty-Bericht-Gezielte-Ueberwachung-von-Menschenrechtler_innen-August-2020.pdf

und deren Auswirkungen) und § 19 Abs. 4 Nr. 1 lit. h BNDG-E (hybride Bedrohungen): Hier wird in keiner Weise näher bestimmt, welche besondere Qualität die bezeichneten Gefahren im Einzelfall haben müssen und von welchen Schäden auszugehen sein muss, um eine strategische Aufklärungsmaßnahme zu rechtfertigen. In ähnlicher Weise gilt dies für die ebenfalls sehr weitgehende Einbeziehung von Gefahren für die Landes- oder Bündnisverteidigung und für Auslandseinsätze der Bundeswehr oder verbündeter Streitkräfte (§ 19 Abs. 4 Nr. 1 lit. a BNDG-E): Die Formulierung definiert die Verteidigung und Auslandseinsätze pauschal als Gefahrenbereich. Statt dessen sollte daran angeknüpft werden, zur Beseitigung welcher Gefahren für ein Gemeinschaftsgut in diesem Bereich (z. B. der Gefahr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland) das Instrument der strategischen Aufklärungsmaßnahme eingesetzt werden darf und welche Schäden für den äußeren oder inneren Frieden Deutschlands damit verbunden sein müssen.

- Die auch vom BVerfG (vgl. Urt. v. 19.5.2020, Rn. 169) geforderte **Begrenzung des erfassten Datenvolumens** je Übertragungsweg kann mit einer **Begrenzung nach der Anzahl der Telekommunikationsnetze nicht erreicht werden**. Die in § 19 Abs. 8 BNDG-E genannte Grenze von 30 Prozent der bestehenden Telekommunikationsnetze ist bereits für sich genommen sehr weit, da sie – insbesondere unter Berücksichtigung des Fortfalls der Inlandsbeschränkung in § 19 Abs. 1 BNDG-E und der expliziten Befugnis zum Hacking ausländischer Telekommunikationsnetze in § 19 Abs. 6 BNDG-E – nur so ausgelegt werden kann, dass sie sich auf alle weltweit bestehenden Telekommunikationsnetze bezieht. Zum anderen besagt eine Beschränkung nach Netzen nichts über die über diese Netze fließenden **Datenmengen**. Schon die Einbeziehung der Backbone-Netze weniger internationaler Tier-1-Provider – deren Kommunikationsverkehr nach diesen Vorgaben dann vollständig überwacht werden dürfte – **kann zu einer Erfassung nahezu sämtlicher internationaler Telekommunikation führen. Dies stellt keine wirksame Begrenzung des Datenvolumens dar, wie sie vom BVerfG intendiert war.** Vielmehr muss die Begrenzung anhand der konkret überwachten Datenmenge definiert werden.

- Auch an einer vom BVerfG geforderten Begrenzung des von der Überwachung abgedeckten **geographischen Gebiets** fehlt es; dass eine solche stattfindet, muss ebenfalls bereits durch den Gesetzgeber sichergestellt werden (BVerfG, Urt. v. 19.5.2020, Rn. 169).

- Die Methoden zur automatisierten **Ausfilterung von Kommunikation unter Beteiligung von Inländern und Deutschen** müssen nach den Vorgaben des BVerfG kontinuierlich fortentwickelt werden und dabei auf dem Stand von **Wissenschaft und Technik** gehalten werden (BVerfG, Urt. v. 19.5.2020, Rn. 173). § 19 Abs. 7 BNDG-E sieht hingegen lediglich vor, dass hierbei der Stand der Technik zu berücksichtigen ist. Dies beschränkt die Fortentwicklungsverpflichtung auf die bereits verfügbaren Filtertechniken und es wird versäumt, dem BND auch die vom BVerfG vorgesehene Pflicht aufzuerlegen, nach dem Stand der Wissenschaft mögliche Fortentwicklungen auch selbst zu betreiben.

- Werden **Daten von Inländern oder Deutschen trotz der Filterung erhoben**, dürfen sie nach § 19 Abs. 7 Satz 4 BNDG-E unter anderem auch dann weiterverarbeitet werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dadurch eine erhebliche Gefahr für die Sicherheit eines anderen EU-, EFTA- oder NATO-Mitgliedstaates abgewendet werden kann. Weder aus dem Gesetzestext noch aus der Begründung ist hinreichend ersichtlich, wie dies mit den **Vorgaben des BVerfG**, das in diesem Zusammenhang lediglich Gefahren für die Sicherheit des Bundes

oder eines Landes benennt, in Einklang gebracht werden kann. Dies gilt auch für andere Regelungen, die auf Gefahren für diese Staaten Bezug nimmt, um bestimmte Maßnahmen ausnahmsweise für zulässig zu erklären, wie etwa die Regelung zur Zulässigkeit gezielter Überwachungsmaßnahmen gegen **Berufsgeheimnisträger** in § 21 Abs. 2 Nr. 2 lit. c BNDG-E und zur Zulässigkeit der Weiterverarbeitung von personenbezogenen Daten, die im Rahmen einer **Eignungsprüfung** erhoben wurden (§ 24 Abs. 7 BNDG-E).

- Die in § 19 Abs. 10 BNDG-E geregelte Differenzierung zwischen den Aufklärungszwecken ist zu grob, um eine zweckgemäße **Verwendungsbeschränkung** herbeiführen zu können. Sie entspricht auch nicht den Anforderungen des BVerfG, das im Rahmen von Aufklärungsmaßnahmen im Sinne von § 19 Abs. 1 Nr. 2 BNDG-E die **Definition von „hinreichend begrenzte(n) und differenzierte(n) Zwecke(n)“** verlangt (vgl. BVerfG, Urt. v. 19.5.2020, Rn. 175). Für jedes erhobene Datum sollte nachgewiesen werden können, zu welchem oder welchen dieser Zwecke die Erhebung erfolgte. Der pauschale Verweis auf die „Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung“ genügt deshalb nicht. Vielmehr ist weitergehend nach den **unter § 19 Abs. 4** benannten, konkreten Aufklärungszwecken zu differenzieren. Daten, die etwa zur Aufklärung terroristischer Gefahren erhoben wurden, dürfen nicht ohne weiteres zur Aufklärung von Angriffen auf kritische Infrastrukturen verwendet werden, wenn dieser Zweck nicht ebenfalls für die konkrete Aufklärungsmaßnahme angegeben wurde. Während § 23 Abs. 3 BNDG-E dies richtigerweise berücksichtigt, fehlt eine Bezugnahme auf die granulareren Aufklärungszwecke im Rahmen der Datenkennzeichnung, wie sie geboten wäre (BVerfG, Urt. v. 19.5.2020, Rn. 182). Auch ist nicht nachvollziehbar, weshalb eine **Kennzeichnung bei Übermittlung entfallen** soll. Im Gegenteil muss gerade bei einer Übermittlung transparent sein, zu welchem Zweck die Daten ursprünglich erhoben wurden und zu welchem Zweck sie nun übermittelt werden, um die Rechtmäßigkeit der Übermittlung auch im Nachhinein überprüfen zu können.

- Die Geltung der Maßgaben in § 19 BNDG für die nachfolgenden Vorschriften ist unklar. Insbesondere in § 20 Abs. 1 und 2 und § 21 Abs. 1 BNDG-E sollte klargestellt werden, dass die Erhebung von Daten von Deutschen auf der Grundlage dieser Vorschrift **nicht zulässig ist**. Denn für diese gelten die Voraussetzungen einer Telekommunikationsüberwachung nach den für Inländer geltenden Vorschriften.

ZUR SOGENANNTEN „EIGNUNGSPRÜFUNG“, § 24 BNDG-E

Die vorgesehenen „Eignungsprüfungen“ geben gleich mehrfach Anlass zur Besorgnis:

- Zum einen handelt es sich bei der Vorschrift um eine Erweiterung der Befugnis zur Erhebung von personenbezogenen Daten über die in § 19 BNDG-E geregelten Grenzen hinaus. Dies ergibt sich jedoch nur mittelbar aus Sinn und Zweck der Regelung und weckt daher Zweifel daran, ob die grundsätzlich abschließende Formulierung in § 19 BNDG-E, die auf die Ausnahmen gemäß § 24 BNDG-E nicht verweist, dem Gebot der **Normenklarheit und Bestimmtheit** entspricht.

- Zum anderen besteht die **erhebliche Gefahr**, dass die Befugnis zur Eignungsprüfung in dem in § 24 BNDG-E geregelten Umfang zu einer letztlich **in wesentlichen Teilen unkontrollierten Dauervollüberwachung der betroffenen Telekommunikationsnetze** mit Blick auf die in § 24 Abs. 7 BNDG-E gestatteten Zwecke führt. Denn anders als in der Vorgängerregelung, die lediglich eine einmalige Anordnung für sechs Monate vorsieht (§ 12 Abs. 2 Satz 3 BNDG), kann die Anordnung gemäß § 24 Abs. 2 Satz 3 BNDG-E **immer wieder um jeweils sechs**

Monate verlängert werden. Ob die Voraussetzungen des § 24 Abs. 1 BNDG-E bei der erstmaligen oder bei einer verlängernden Anordnung tatsächlich vorliegen, kann durch den Unabhängigen Kontrollrat **nicht überprüft** werden, da dieser nicht hierfür nicht zuständig ist (vgl. § 42 BNDG-E). Damit hängt die Durchführung und potentiell dauerhafte Verlängerung einer Eignungsprüfung für ein bestimmtes Telekommunikationsnetz allein von der Entscheidung der nach § 24 Abs. 3 BNDG-E zur Anordnung befugten Personen – also einer **allein BND-internen Entscheidung** - ab. Die sogenannte Eignungsprüfung wird somit zum potentiellen Einfallstor für eine der Kontrolle entzogene anlasslose Massenüberwachung.

- Gegenüber der Vorgängerregelung wurden zudem die Fälle, in denen die Daten aus Eignungsprüfungen **weiterverarbeitet** werden dürfen, beträchtlich erweitert. Gemäß § 24 Abs. 7 Abs. 1 BNDG-E dürfen Daten schon dann weiterverarbeitet werden, wenn tatsächliche Anhaltspunkte für eine erhebliche Gefahr für die in lit. a und b genannten Rechtsgüter bestehen. Weder ist Voraussetzung, dass sich diese tatsächlichen Anhaltspunkte aus den im Rahmen der Eignungsprüfung erhobenen Daten ergeben, noch muss die Weiterverarbeitung (anders als noch gemäß der Vorgängerregelung in § 12 Abs. 5 BNDG) irgendeinen Beitrag zur Abwendung dieser Gefahr leisten. Eine derart unbestimmte Formulierung dürfte den Anforderungen an eine **normenklare und präzise** Eingriffsregelung nicht entsprechen. Über die Vorgängerregelung hinaus geht ferner die hinzugefügte Befugnis zur **Übermittlung der Daten an die Bundeswehr**, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies zum Schutz bestimmter Rechtsgüter erforderlich ist (§ 24 Abs. 7 Nr. 2 BNDG-E). Diese Übermittlung darf gemäß § 24 Abs. 7 Satz 2 BNDG-E auch automatisiert erfolgen. Es fehlen jedoch Maßgaben dazu, wie im Rahmen einer automatisierten Übermittlung effektiv geprüft werden soll, ob tatsächliche Anhaltspunkte für eine Erforderlichkeit zum Schutz dieser Rechtsgüter vorliegen. Schließlich erlaubt § 24 Abs. 6 Satz 2 BNDG-E die **fortdauernde Speicherung von Daten**, deren Inhalt für den BND nicht lesbar ist und die zu Forschungszwecken benötigt werden, für einen Zeitraum von zehn Jahren. Hierzu dürfte sämtliche mithilfe eines zum Erhebungspunkt als sicher eingestuften Algorithmus verschlüsselte Kommunikation zählen. Eine nähere Bestimmung der Forschungszwecke, zu denen von einer Löschung der Daten nach Ablauf der in § 24 Abs. 6 Satz 1 BNDG-E geregelten Fristen abgesehen werden kann, fehlt. Auch ist nicht ersichtlich, auf welche Rechtsgrundlage sich der BND bei der weiteren Verarbeitung dieser Daten zu den nicht näher spezifizierten Forschungszwecken stützen kann. Auch die Weiterverarbeitungsbefugnisse **unterliegen nicht der Kontrolle** durch den Unabhängigen Kontrollrat.

- Schließlich besteht die Gefahr, dass mit der Eignungsprüfung die **Beschränkung der Ausland-Fernmeldeaufklärung auf 30 Prozent der bestehenden Telekommunikationsnetze (§ 19 Abs. 8 BNDG-E) umgangen** werden kann. Denn diese Quote findet keine Anwendung auf die für die Durchführung der Eignungsprüfung ausgewählten Telekommunikationsnetze. Auch eine andere quantitative Schranke für die Erhebung und Auswertung personenbezogener Daten aus Telekommunikationsnetzen zur Eignungsprüfung ist nicht ersichtlich.

UMGEHUNG DES VERBOTS DER ERHEBUNG VON VERKEHRSDATEN VON DEUTSCHEN UND INLÄNDERN

Die Regelung in § 26 Abs. 3 Satz 2 BNDG-E stellt **eine unzulässige Umgehung des grundsätzlichen Verbots der Erhebung von Verkehrsdaten von Deutschen und Inländern** dar:

- Nummer 1 erlaubt die Verarbeitung von personenbezogenen Verkehrsdaten, die trotz ihres Personenbezugs "ohne unmittelbaren Bezug zu einem konkreten menschlichen

Kommunikationsvorgang anfallen". Eine derartige Differenzierung ist nach den **Vorgaben des BVerfG unzulässig** und würde zu einer Erhebung personenbezogener Daten über Deutsche oder Inländer führen, die von vornherein "mit allen zur Verfügung stehenden technischen Mitteln technisch herausgefiltert und spurenlos gelöscht werden müssen, bevor eine manuelle Auswertung erfolgt" (BVerfG Rn. 173). Soweit eine solche Filterung technikbedingt eine Datentrennung nicht vollständig gewährleisten kann, dürfen die Daten von Deutschen oder Inländern nicht genutzt werden und sind unverzüglich zu löschen (Rn. 174). Dies steht einer weiteren Verarbeitung entgegen.

- Nummer 2 erlaubt die **Verarbeitung von personenbezogenen Verkehrsdaten von Deutschen und Inländern** ohne Einschränkung, soweit sie unverzüglich nach ihrer Erhebung automatisiert unkenntlich gemacht werden. Dies **widerspricht den Vorgaben des BVerfG**, nach denen bereits die Erhebung von Verkehrsdaten, die sich auf Deutsche oder Inländer beziehen, unzulässig ist, soweit die Ausfilterung technisch möglich ist. Nummer 2 differenziert jedoch nicht nach der technischen Möglichkeit einer Ausfilterung, sondern erlaubt die Erhebung ohne Einschränkung. Auch soweit Verkehrsdaten selbst mit allen zur Verfügung stehenden Mitteln technisch nicht herausgefiltert werden können und deshalb zunächst erhoben werden dürfen, dürfen sie anschließend "nicht genutzt werden und sind unverzüglich zu löschen" (Rn. 174). Selbst wenn man in einer Anonymisierung eine zulässige Form der Löschung personenbezogener Daten sähe, ist darauf hinzuweisen, dass eine Anonymisierung, die den in § 26 Abs. 3 Satz 3 BNDG-E aufgestellten Anforderungen genügt, dem BND in vielen Fällen nicht gelingen dürfte. Denn er verfügt über weitreichende Befugnisse zur Erhebung weiterer Daten, die zur **Identifizierung der betroffenen Personen** – ggf. durch Kombination der Datensätze – führen können.

ÜBERPRÜFUNG DER ERFORDERLICHKEIT DER SPEICHERUNG PERSONENBEZOGENER INHALTSDATEN

- Der in § 27 Abs. 1 Satz 1 BNDG-E vorgesehene Zeitraum für die Überprüfung überschreitet nach Ansicht von Amnesty die Grenzen der **Verhältnismäßigkeit** bei Weitem. Eine Überprüfung des fortdauernden Bestehens eines die Erhebung rechtfertigenden Zwecks gemäß § 19 Abs. 1 BNDG-E hat **laufend und in kurzen Zeitabständen** zu erfolgen, um sicherzustellen, dass Daten nicht länger als erforderlich gespeichert werden.

ÜBERMITTLUNG VON PERSONENBEZOGENEN DATEN AN INLÄNDISCHE STELLEN, §29 BND-GE

- Die in § 29 Abs. 1 Nr. 1 und 2, Abs. 2, Abs. 3, Abs. 4 Nr. 2, Abs. 5, Abs. 6, Abs. 7, Abs. 8 Nr. 2 BNDG-E verwendete Formulierung, nach der Voraussetzung für eine Übermittlung sein soll, dass "tatsächliche Anhaltspunkte" dafür bestehen, dass diese zum Schutz bestimmter Rechtsgüter erforderlich sei, entspricht nicht den Vorgaben des BVerfG, das im Rahmen der verfassungsrechtlichen Verhältnismäßigkeitsprüfung verlangt, dass die Übermittlung zur Erreichung eines legitimen Zwecks **tatsächlich erforderlich** ist (vgl. BVerfG, Rn. 216), und es nicht genügen lässt, dass hierfür lediglich tatsächliche Anhaltspunkte vorliegen. Das Vorliegen tatsächlicher Anhaltspunkte kann vielmehr nur bei der Beurteilung eine Rolle spielen, ob eine hinreichend konkret absehbare Gefahrenlage besteht, die die Übermittlungsschwelle überschreitet: Als Mindestvoraussetzung müssen hierfür tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen (BVerfG, Rn. 222). Hierauf bezieht sich die Gesetzesformulierung jedoch nicht. Der Wortlaut ist daher anzupassen, um die vom BVerfG konkretisierten verfassungsrechtlichen Maßgaben umzusetzen. Andernfalls würde die Übermittlungsbefugnis über die Fälle hinaus ausgedehnt, bei denen die Übermittlung zum Schutz der benannten Rechtsgüter tatsächlich erforderlich ist.

- § 29 Abs. 1 Nr. 2 BNDG-E **umfasst die Weitergabe von Daten an BfV, Verfassungsschutzbehörden der Länder und MAD** zum Zweck der Unterrichtung der Bundes- oder einer Landesregierung und erlaubt dies schon dann, "wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies zur Erfüllung seiner Aufgaben oder der Aufgaben der Empfänger erforderlich ist". Das BVerfG gestattet indes eine **Übermittlung ohne besonders qualifizierte Anforderungen** an Rechtsgüterschutz und Übermittlungsschwellen **lediglich an die Bundesregierung** (BVerfG Rn. 223 ff.) und nur, soweit dies "zur Wahrnehmung ihrer außen- und sicherheitspolitischen Verantwortung" (Rn. 223) erfolgt. Die Pflege der auswärtigen Beziehungen ist jedoch Aufgabe des Bundes (Art. 32 Abs. 1 GG). Im Bereich der Außen- und Verteidigungspolitik steht dem Bund die ausschließliche Gesetzgebungskompetenz zu (Art. 72 Abs. 1 Nr. 1 GG). Schon aus diesem Grund kann eine Übermittlung zum Zweck der Unterrichtung einer Landesregierung ohne zusätzliche Voraussetzungen nicht zulässigerweise erfolgen, unabhängig davon, ob die Daten mit dem Zweck der politischen Unterrichtung oder der Gefahrenfrüherkennung gekennzeichnet wurden.

- Erst recht gilt das unter dem vorangegangenen Aufzählungspunkt Gesagte hinsichtlich der in § 29 Abs. 2 BNDG-E enthaltenen Befugnis einer **Übermittlung** von Daten zu dem genannten Zweck **an andere inländische öffentliche Stellen**, deren Aufgaben mangels konkreter Benennung nicht eingrenzbar sind. Eine derart weite Befugnisnorm dürfte daher nicht nur **gegen den Grundsatz der Verhältnismäßigkeit, sondern schon gegen das Erfordernis einer "normenklaren und hinreichend bestimmten Rechtsgrundlage" (**Rn. 213; BVerfGE 65, 1, 46; vgl. insb. BVerfGE 100, 313, 389) verstoßen.

- § 29 Abs. 4 BNDG-E ist in mehrerlei Hinsicht **zu unbestimmt formuliert**, um den verfassungsrechtlichen Anforderungen an die Bestimmtheit der Eingriffsnorm gerecht zu werden: Zum einen ergibt sich aus der Verweisung auf Absatz 2 nicht, ob damit sämtliche inländischen öffentlichen Stellen bezeichnet werden sollen oder nur solche, an die der BND auch unter den weiteren Voraussetzungen des Absatzes 2 Daten übermitteln darf. Zum anderen gestattet § 29 Abs. 4 Nr. 1 BNDG-E die Übermittlung, "soweit dies in anderen Rechtsvorschriften vorgesehen ist", ohne diese Rechtsvorschriften jedoch hinreichend klar zu benennen. Das BVerfG verlangt, "Verweisungen [müssen] begrenzt bleiben, 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" (Rn. 215). Durch die offene Formulierung besteht die Gefahr einer **uferlosen Verweisung** auf eine Vielzahl bestehender und möglicherweise erst künftig entstehender Normen, deren Gesamtzahl kaum eingrenzbar ist und deren Anwendbarkeit sich nicht in allen Fällen ohne erhebliche Schwierigkeiten erschließt.
- § 29 Abs. 5 Satz 2 BNDG-E erlaubt die Übermittlung von Daten an die **Bundeswehr** unter bestimmten Voraussetzungen auch **automatisiert**. Dies erscheint grundrechtlich bedenklich, da zweifelhaft ist, wie die erforderliche **Prüfung des Vorliegens der Übermittlungsvoraussetzungen bei einer automatisierten Übermittlung sichergestellt** werden kann. Allein die Einschränkung auf Daten, die im Rahmen von Aufklärungsmaßnahmen nach § 19 Abs. 4 Nr. 1 lit. a oder Nr. lit. a BNDG-E erhoben wurden, kann nicht hinreichend sicher gewährleisten, dass auch die Übermittlung dieser Daten an die Bundeswehr verfassungsrechtlich gerechtfertigt ist.

- Die in § 29 Abs. 6 Satz 3 BNDG-E geregelte Übermittlungsbefugnis entspricht in ihrer Ausgestaltung nicht den vom BVerfG definierten verfassungsrechtlichen Anforderungen an Übermittlungen durch den BND. Die Regelung enthält **weder eine Begrenzung hinsichtlich der Rechtsgüter**, zu deren Schutz die Übermittlung erfolgt, noch eine nennenswerte **Beschränkung**

hinsichtlich der Übermittlungsschwelle, die überschritten sein muss. Es ist nicht ersichtlich, weshalb die Intensität des dadurch bewirkten Grundrechtseingriff nur deshalb geringer sein soll, weil die Daten zur Konkretisierung einer Anfrage an eine andere Stelle dienen, der die Daten bereits bekannt sind, wenn die Daten der ersten Stelle vor der Übermittlung nicht bekannt sind. Entsprechend kann auch hinsichtlich der Anforderungen an eine Rechtfertigung der Übermittlung kein anderer Maßstab gelten als für eine Übermittlung in den übrigen in § 29 BNDG-E genannten Konstellationen. Überdies dürfte die Bezugnahme auf eine "Anfrage an eine andere Stelle" aufgrund ihrer Weite und Unschärfe weder dem Gebot der **Normenklarheit noch dem Prinzip der Verhältnismäßigkeit** entsprechen, da sich aus den verwendeten Begriffen keine taugliche Eingrenzung der Sachverhalte ergibt, auf die die Norm Anwendung finden soll.

- § 29 Abs. 15 BNDG-E sollte um eine **Klarstellung ergänzt** werden, durch die effektiv verhindert wird, dass es unter Hinweis auf behauptete Unvollständigkeiten bereits übermittelter Daten zu weitreichenden **dauerhaften Übermittlungen weiterer Daten** an den Empfänger kommt, zu deren Übermittlung der BND nach den § 29 Abs. 1-7 BNDG-E nicht befugt wäre (z. B. weil der Übermittlungszweck für diese Daten nicht oder nicht mehr vorliegt).

ÜBERMITTLUNG VON PERSONENBEZOGENEN DATEN AN AUSLÄNDISCHE, ÜBER- UND ZWISCHENSTAATLICHE STELLEN

- Wie bereits oben zu § 29 Abs. 1 Nr. 1 und 2, Abs. 2, Abs. 3, Abs. 4 Nr. 2, Abs. 5, Abs. 6, Abs. 7, Abs. 8 Nr. 2 BNDG-E angemerkt, stellt die Anforderung, nach der "tatsächliche Anhaltspunkte" dafür bestehen müssen, dass eine Übermittlung zum Schutz bestimmter Rechtsgüter erforderlich sei, aus Sicht von Amnesty keine ausreichende Übermittlungsschwelle dar. Die **Forderung nach einer Wortlautanpassung erstreckt sich** folglich auch auf die Verwendung der Formulierung in § 30 Abs. 1, Abs. 2, Abs. 3, Abs. 4 und Abs. 5 BNDG-E.

- Die zu § 29 Abs. 1 Nr. 2 und Abs. 2 BNDG-E geäußerte Kritik hinsichtlich des Fehlens hinreichend qualifizierter Anforderungen an **Rechtsgüterschutz und Übermittlungsschwellen** gilt auch für die insoweit gleichlaufende Bestimmung in § 30 Abs. 1 BNDG-E.

- Die zu § 29 Abs. 6 Satz 3 BNDG-E geäußerte Kritik hinsichtlich des Fehlens hinreichend qualifizierter Anforderungen an **Rechtsgüterschutz und Übermittlungsschwellen und des Verstoßes gegen das Gebot der Normenklarheit** gilt ebenso für die entsprechende Regelung einer Übermittlung an ausländische Stellen gemäß § 30 Abs. 4 Satz 4 BNDG-E.

- Die Regelung in § 30 Abs. 6 BNDG-E, aus der sich ergibt, **in welchen Fällen Daten nicht an ausländische Stellen weitergegeben werden dürfen**, bleibt hinter den Anforderungen des BVerfG an die normenklare gesetzliche Regelung einer **Rechtsstaatlichkeitsvergewisserung** zurück (BVerfG, Rn. 238 ff.). Die Vorschrift erlegt dem BND **keinerlei aktive Vergewisserungspflicht auf**, sondern macht die Prüfung der Rechtsstaatlichkeitsanforderungen davon abhängig, dass das Überwiegen von schutzwürdigen Interessen des Betroffenen für den BND "erkennbar" ist. Die insoweit sehr detaillierten Vorgaben des BVerfG zum Verfahren und der abgestuften materielle Prüftiefe (einschließlich der Pflicht zur Durchführung einer betroffenenspezifischen Prüfung und einer eigenständigen Abwägung bei Daten aus Vertraulichkeitsbeziehungen), sind im Gesetzentwurf **nur unzureichend berücksichtig**t. Auch die Pflicht zur Prüfung des Datenschutzniveaus hat in die Regelung in § 30 Abs. 6 BNDG-E nicht in ausreichender Klarheit Eingang gefunden. Insbesondere die Gewährleistung der Einhaltung von Grundsätzen der Verarbeitung personenbezogener Daten wie des

Zweckbindungsgrundsatzes und des Grundsatzes der Datenminimierung **stellt eine fundamentale Schutzvorkehrung zugunsten des Betroffenen dar, die das BVerfG (Rn. 236) für jede Übermittlung an ausländische Staaten fordert, die sich aus § 30 Abs. 6 BNDG-E jedoch nicht ergibt**. Dadurch besteht die Gefahr, dass sich der BND bei der Übermittlung von Daten an ausländische Stellen nicht im gebotenen Umfang von dem im betreffenden ausländischen Staat bestehenden Datenschutzniveau leiten lässt und lediglich "(i)n Zweifelsfällen" verbindliche diesbezügliche Zusicherungen berücksichtigt (§ 30 Abs. 6 Satz3 BNDG-E). Die Regelung kann die Betroffenen auch nicht hinreichend vor möglichen weiteren **Menschenrechtsverletzungen** in Folge der Weitergabe sie betreffender Daten an eine ausländische Stelle schützen.

EINGRIFF IN INFORMATIONSTECHNISCHE SYSTEME VON AUSLÄNDERN IM AUSLAND (ONLINE-DURCHSUCHUNG UND QUELLEN-TKÜ), § 34 BNDG-E

Durch § 34 BNDG-E soll der BND künftig die Befugnis erhalten, im Rahmen einer angeordneten gezielten Überwachungsmaßnahme die Datenerhebung mit Hilfe der Online-Durchsuchung und der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) durchzuführen. Derartige Maßnahmen erfordern die Überwindung der Integrität des informationstechnischen Systems (IT-Systems), von dem die Daten erhoben werden sollen, durch technische Mittel (Hacking). Damit verbunden sind besonders intensive Eingriffe in Grund- und Menschenrechte, insbesondere das Recht auf Achtung des Privatlebens. Aus Sicht von Amnesty bestehen **erhebliche grundsätzliche Zweifel an der Verhältnismäßigkeit eines Einsatzes derartiger Technologien im Rahmen der Vorfeldaufklärung**:

- **Unverhältnismäßig** ist aus Sicht von Amnesty jedenfalls der Rückgriff auf eine solche Maßnahme im Bereich der politischen Unterrichtung der Bundesregierung (§ 34 Abs. 1 Satz 1 Nr. 1 BNDG-E), in dem es **nicht um die Aufklärung einer abstrakten Gefahrenlage** geht, die von der betroffenen Person ausgeht, sondern **lediglich um das Interesse der Bundesregierung, über Geschehnisse und Situationen von außen- und sicherheitspolitischer Bedeutung informiert** zu werden. Auch die durch § 34 Abs. 2 BNDG-E vorgesehene Beschränkung auf Informationen von "herausgehobener außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland" kann am grundsätzlichen Überwiegen der Rechte der betroffenen Person nichts ändern. Lediglich ergänzend ist darauf hinzuweisen, dass der Wortlaut schon zu **unbestimmt** ist, um die grundlegende Anforderung an eine hinreichend klare und präzise gesetzliche Grundlage zu erfüllen: Ein Maßstab, der zur Beurteilung der "Herausgehobenheit" herangezogen werden könnte, ist auch aus der Begründung zum Gesetzentwurf nicht ersichtlich; der Begriff wird neben § 34 BNDG-E an keiner anderen Stelle im BNDG verwendet.

- Gemäß § 34 Abs. 1 Satz 1 Nr. 2 BNDG-E ist der Eingriff in IT-Systeme und die Datenerhebung aus ihnen ebenfalls zulässig, wenn dies erforderlich ist zur "**Früherkennung** von aus dem Ausland drohenden Gefahren von internationaler Bedeutung". Es erscheint nur schwer vorstellbar, dass der Einsatz eines derart eingriffsintensiven Instruments wie dem der Quellen-TKÜ - erst recht nicht dem der Online-Durchsuchung - so weit im Vorfeld einer konkreten Gefahr bei einer Abwägung der damit verfolgten legitimen Ziele im Aufgabenbereich des BND mit den gewichtigen grundrechtlichen Positionen der betroffenen Personen **als verhältnismäßig gerechtfertigt werden kann**. Auch in diesem Kontext genügt die Beschränkung auf "Fälle von herausgehobener außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland" gemäß § 34 Abs. 3 BNDG-E weder den Anforderungen an eine **normenklare und hinreichend bestimmte** gesetzliche Regelung noch an die Definition **substantieller Eingriffsschwellen**, die dem Eingriffsgewicht der Maßnahme Rechnung tragen.

- Unabhängig von den genannten grundsätzlichen Zweifeln an der Verhältnismäßigkeit der Maßnahmen im Aufgabenbereich des BND sind an ihre Anordnung und Durchführung unter Zugrundelegung internationaler Menschenrechtsstandards dringend **zusätzliche Anforderungen** zu stellen, die bislang im BNDG-E keinen Niederschlag gefunden haben:

    - Die **Anordnung** gemäß § 37 Abs. 1 BNDG-E muss die betroffene Person bzw. das Zielsystem **konkret benennen**. Obwohl die Anforderungen in § 34 Abs. 2, 3 und 5 BNDG-E voraussetzen, dass diese Angaben vorliegen, wird die Benennung in der Anordnung nach dem Wortlaut des § 37 Abs. 2 BNDG-E nicht ausdrücklich gefordert.
    - Die **technischen und organisatorischen Maßnahmen** zur Gewährleistung eines den Grundsätzen der Verhältnismäßigkeit genügenden Eingriffs sind nach Einschätzung von Amnesty nur unzureichend definiert. Die in § 34 Abs. 4 BNDG-E beschriebenen Anforderungen an die Vornahme der erforderlichen technischen Modifikationen des Zielsystems können nicht sicherstellen, dass die Daten unverfälscht erhoben werden. Gerade in einem System, dessen Integrität von außen durch technische Mittel überwunden werden kann, kann eine **Verfälschung der Daten durch Dritte bzw. das kompromittierte Zielsystem selbst nicht ausgeschlossen werden**. Es **bedarf daher zusätzlicher Maßnahmen**, mit denen die Manipulationssicherheit bestmöglich gewährleistet wird bzw. sichergestellt ist, dass verbleibende Unsicherheiten aufgrund nachfolgender Maßnahmen nicht zu Lasten der betroffenen Person gehen:
    - Die **Mindestanforderungen an die Protokollierung** in anderen Gesetzen, die eine Befugnis zur Online-Durchsuchung vorsehen, sind auch hier einzuhalten. Hierzu sollte der Wortlaut von § 100a Abs. 6 StPO in die Regelung des § 34 BNDG-E aufgenommen werden.
    - Die Protokollierung sollte **revisionssicher** sein und über die Anforderungen in § 100a Abs. 6 StPO hinaus auch sämtlicher Schritte **bei der Anwendung** des technischen Mittels umfassen, um eine lückenlose Überprüfung des Handelns seitens der Behörde zu ermöglichen. Erhobene Daten müssen unverzüglich nach der Erhebung **in unveränderlicher Weise gespeichert** werden; die Manipulationsfreiheit sollte durch geeignete Maßnahmen (z. B. durch Verwendung einer Prüfsumme) dokumentiert werden. Das verwendete technische Mittel muss gewährleisten, dass unzulässige Eingriffe in die Funktionsweise durch Dritte nach dem Stand der Technik ausgeschlossen sind.
    - Es sollte organisatorisch sichergestellt sein, dass die **Evaluation** der erhobenen Daten das verbleibende Manipulationsrisiko hinreichend berücksichtigt. Insbesondere dann, wenn Daten an andere in- oder ausländische Stellen weitergegeben werden sollen, die auch operative Befugnisse haben, muss sichergestellt sein, dass die Aussagekraft und ggf. der Beweiswert der erhobenen Daten in Anbetracht dieses Risikos bewertet werden.
    - Die **Anordnung** gemäß § 37 Abs. 1 BNDG-E muss das zur Durchführung der Maßnahme vorgesehene **technische Mittel konkret benennen**, um sicherzustellen, dass nur technische Mittel zum Einsatz kommen, die die grund- und menschenrechtlichen Anforderungen erfüllen.
    - Es muss sichergestellt werden, dass die Beurteilung der Verhältnismäßigkeit einer **Ausnutzung von geheim gehaltenen Sicherheitslücken** zur Ermöglichung der Maßnahme nach einem Prozess zum **Schwachstellenmanagement** erfolgt, also eines Prozesses, der die Verhältnismäßigkeit der Ausnutzung einer Schwachstelle prüft und dabei die damit verbundenen **Risiken einer fortdauernden Geheimhaltung für die**

Allgemeinheit angemessen berücksichtigt. Der Prozess sollte vorsehen, dass bekannte Sicherheitslücken nach einem anerkannten Verfahren **frühestmöglich veröffentlicht** werden. **Amnesty setzt sich für zahlreiche Menschenrechtsverteidiger_innen weltweit ein, deren Kommunikation unter Ausnutzung nicht bekannter Sicherheitslücken überwacht wurde und wird.**[3] Angesichts potentiell globaler Auswirkungen ist Amnesty der Auffassung, dass die Ausnutzung bisher unbekannter Schwachstellen – wenn überhaupt – nur dann zulässig sein kann, wenn ein Schwachstellenmanagement etabliert wurde.

"GERICHTSÄHNLICHKEIT", SCHUTZ VON MENSCHENRECHTEN UND STÄRKUNG DER BETROFFENENPERSPEKTIVE BEI DER KONTROLLE

- Um die vom Bundesverfassungsgericht geforderte **"Gerichtsähnlichkeit"** der Kontrolle zu erreichen und menschenrechtliche Erwägungen bei der Entscheidung über Überwachungsvorgänge in der Praxis zu stärken, bedarf es dringend einer **Stärkung der Perspektive der von Überwachung Betroffenen.** Da das gerichtsähnliche Organ mögliche Anordnungen des BND prüft, liegt ihm naturgemäß erst einmal **nur die Perspektive des BND** vor. Die teilweise Besetzung des Organs mit **Bundesanwält_innen** könnte diese Perspektive tendenziell noch verstärken. **Daher sollte ein kontradiktorisches Verfahren eingeführt werden.** Dies ist auch mit der derzeit geplanten Besetzung des Organs möglich, das Gremium würde aber deutlich von der expliziten Aufnahme eines **"Anwalts/Anwältin der Menschenrechte"** profitieren, der/die über einen entsprechenden fachlichen Hintergrund verfügt.

- Wie in der dem Entwurf vorausgehenden Debatte wiederholt vorgeschlagen, sollte dem Kontrollrat zudem ein **Expert_innenbeirat** zur Seite gestellt werden. Dieser sollte insbesondere über technische Expertise verfügen sowie über Kenntnisse der **Grund- und Menschenrechte und ihrer Lage in den Ländern, die Objekt der Aufklärung, und in denen, die Partner der nachrichtendienstlichen Zusammenarbeit und Zielländer von Datenübermittlungen** sind. Auch eine verstärkte technische Expertise ist notwendig, um es dem Kontrollrat zu ermöglichen, Selektoren zu beurteilen, die oft in ohne technische Expertise nicht lesbarer Form vorliegen.

BENACHRICHTIGUNGEN UND ZUGANG ZU EFFEKTIVEN RECHTSMITTELN

- Internationale Menschenrechtsstandards machen es aus Sicht von Amnesty erforderlich, dass - anders als in § 59 Abs. 1 BNDG-E vorgesehen - auch im Kontext von Überwachungsmaßnahmen, die sich im Ausland aufhaltende Ausländer betreffen, eine **Benachrichtigung der von der Maßnahme betroffenen Personen** zu erfolgen hat, sobald dies möglich ist, ohne den Erfolg der Maßnahme zu gefährden. Die Benachrichtigung muss auch eine Begründung für die Maßnahme und die erhobenen Daten enthalten und statthafte Rechtsbehelfe gegen die Maßnahme benennen. Soll **von der Benachrichtigung abgesehen** werden, ist dies von einer gerichtsähnlichen Stelle (z. B. dem gerichtsähnlichen Kontrollorgan des Unabhängigen Kontrollrats) **zu genehmigen.**

- Den betroffenen Personen müssen darüber hinaus **effektive Rechtsmittel** zur Verfügung stehen, um gegen Menschenrechtsverletzungen durch die Ausübung der eingeräumten Befugnisse vorgehen zu können. **Diese fehlen im Gesetzentwurf bislang völlig** und können aus Sicht von

[3] Siehe Amnesty International, Bericht „Gezielte Überwachung von Menschenrechtsverteidigern“, 2020, online: https://www.amnesty.de/sites/default/files/2020-09/Amnesty-Bericht-Gezielte-Ueberwachung-von-Menschenrechtler_innen-August-2020.pdf

Amnesty unter menschenrechtlicher Perspektive auch nicht durch eine institutionalisierte gerichtsähnliche Kontrolle kompensiert werden.

LÜCKEN DER KONTROLLE DURCH DEN KONTROLLRAT

- Dem gerichtsähnlichen Kontrollorgan sollen nach BND-GE keine Suchmerkmale (Selektoren) zur Prüfung mit vorgelegt werden. Damit bleibt die Prüfung von Anordnungen unvollständig, denn ohne Kenntnis der Selektoren ist schwer einzuschätzen, ob eine Maßnahme geeignet und verhältnismäßig ist. **Dringend sollten daher Selektoren in den Prüfumfang mit aufgenommen werden.** Unklar bleibt im BND-GE, ob und wann das administrative Kontrollorgan eine Selektorenprüfung vornehmen kann, wenn die "originäre Zuständigkeit" des gerichtsähnlichen Kontrollorgans berührt ist, dem die Selektoren jedoch nicht vorgelegt wurden. Auch wenn der administrativen Kontrolle hier ein Einblick möglich ist, kann sie doch **kaum überprüfen**, ob die verwendeten Selektoren im Sinne der vom gerichtsähnlichen Kontrollorgan genehmigten Anordnung sind, wenn Selektoren kein Teil dieser Anordnung waren. Es ist daher unklar, worauf (von Extremfällen abgesehen) sich eine solche Prüfung von Selektoren durch die administrative Kontrolle beziehen soll.

- Eine weitere Kontrolllücke stellt in §56 BND-GE der Bereich der **internationalen Kooperationen** dar, sofern die IT-Systeme nicht der alleinigen Verfügungsbefugnis des BND unterliegen. Zwar findet sich hierfür eine Angabe in der Begründung (das Kopieren der betroffenen Daten in eine BND-eigene Datei, vgl. S.113 BND-GE), die jedoch auch **explizit in den Gesetzestext aufgenommen** werden sollte. Dieser enthält selbst nur die vage Formulierung, dass das Bundeskanzleramt in diesen Fällen „geeignete Maßnahmen“ ergreife. Zusätzlich sollte ausdrücklich vorgesehen werden, dass der Kontrollrat über solche Systeme **automatisch unterrichtet** wird, da aus dem Text nicht ersichtlich wird, ob das Kopieren nur auf Bitte des Kontrollrates erfolgt (der dafür erst einmal Kenntnis der gemeinsam geführten Dateien haben müsste) oder proaktiv.

- Dass der potentiell umfangreiche Bereich der **Eignungsprüfungen** nach §24 BND-GE der Kontrolle durch den Kontrollrat gänzlich entzogen ist, ist unverständlich, unbedingt sollte – wie bereits dargelegt - **auch die Eignungsprüfung einer Kontrolle durch beide Organe des Unabhängigen Kontrollrates unterworfen** werden.

ERSCHWERTE MÖGLICHKEIT DER BEANSTANDUNGEN UND FEHLENDE SANKTIONSMÖGLICHKEITEN DURCH KONTROLLRAT UND BFDI

- Der Weg zu einer Beanstandung durch den Kontrollrat dauert **deutlich zu lange** und ist durch seine verschiedenen Schritte für den Kontrollrat enorm arbeitsintensiv. Durch diese Schritte, darunter mehrere Möglichkeiten zur Stellungnahme durch das Bundeskanzleramt, das hierbei teilweise drei Monate Zeit für eine Antwort hat, ergibt sich ein **potentiell mehrmonatiger Prozess**. Es steht zu befürchten, dass in diesem Zeitraum beispielweise ein **unrechtmäßiger Überwachungsprozess vollständig durchgeführt, ausgewertet und abgeschlossen werden** kann,

ohne dass der Kontrollrat dies unterbinden könnte. Dies eröffnet auch die Möglichkeit von **Missbrauch**. Es bleibt zudem unklar, ob der Kontrollrat im Falle erfolgter Beanstandungen über weitere Sanktionsmöglichkeiten verfügt. Der Prozess sollte entschlackt, die mögliche Antwortfrist des Bundeskanzleramts verkürzt und **Sanktionsmöglichkeiten vorgesehen** werden.

- Eine Aufnahme von **Sanktionsmöglichkeiten wäre auch für den BfDI** im Bereich der Nachrichtendienste wünschenswert, dem im BND-GE bedauerlicherweise weiterhin keine Möglichkeit für **konkrete Anordnungsbefugnisse** eingeräumt wird, wie sie etwa das BKA-Gesetz vorsieht. Der BfDI bleibt damit auf das vergleichsweise schwache Instrument der Beanstandungen beschränkt.

FRAGMENTIERUNG DER KONTROLLE

- Leider hat sich die Bundesregierung dagegen entschieden, die Fragmentierung der Nachrichtendienstkontrolle zu reduzieren, und im Gegenteil mit dem unabhängigen Kontrollrat eine weitere Instanz mit zwei Organen geschaffen. Grundsätzliche **Schwierigkeiten der Fragmentierung - Kontrolllücken bei zugleich anderweitigen Doppelzuständigkeiten, mangelhafter Austausch, Risiko blinder Flecken und eines "Zuschauereffektes"** (Annahme, eine andere Instanz kontrolliere) - bleiben daher bestehen. So werden in Zukunft mit neuem Kontrollrat und G10-Kommission zwei sehr unterschiedliche Gremien teils sehr ähnliche Aufgabenfelder kontrollieren. Obwohl dies zwischenzeitlich zur Debatte stand, sind die neu hinzukommenden administrativen Kontrollkompetenzen auch nicht dem Bundesdatenschutzbeauftragten (BfDI) übertragen worden. Möglicherweise kommt es hierdurch in Zukunft zu Doppelungen bei einzelnen Kontrollvorgängen, denn die Zuständigkeiten sind im Detail nicht klar abgegrenzt. Es ist deshalb zu begrüßen und dringend notwendig, dass es nach §58 BND-GE dem BfDI, der G10-Komission und dem neuen Kontrollrat künftig wenigstens möglich sein soll, sich **auszutauschen**, auch, um einen "Zuschauereffekt" zu vermeiden und um Erfahrungen und Fragen auszutauschen.

- Defizite einer Fragmentierung verstärken sich innerhalb des neuen Kontrollrates, wenn die Kompetenzen des administrativen Kontrollorgans dort eingeschränkt werden, wo **"originäre Zuständigkeiten" des gerichtsähnlichen Kontrollorgans berührt** würden. Dies könnte zu unnötiger Verwirrung und Rückzug der administrativen Kontrolle aus bestimmten Bereichen führen.

- **Praktische Beispiele** für einen verbesserten Austausch und eine verstärkte Zusammenarbeit der verschiedenen Kontrollorgane hat die Stiftung Neue Verantwortung zusammengestellt. Sie nennt in ihrer Stellungnahme zum BND-Gesetzentwurf etwa "gemeinsame Schulungen, gemeinsam abgestimmte Prüfaufträge, gemeinsam genutzte Ressourcen (technisch geschultes Personal, Expertenbeiräte), abgestimmte Prioritätensetzung bei der Jahresplanung der Kontrolltätigkeiten, gemeinsame Evaluationen, gemeinsame Berichterstattungen und

Austausch von Personal zur Weitergabe von Prüferfahrungen und Fachwissen."[4] Alle zitierten Vorschläge **unterstützt Amnesty International explizit**.

[4] Kilian Vieth; Thorsten Wetzling: Stellungnahme im Rahmen der Verbändebeteiligung zum Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts und des Bundesverwaltungsgerichts, 3. Dezember 2020, Berlin