Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Vorsitzende des
Ausschusses für Inneres und Heimat
des Deutschen Bundestages
Frau Andrea Lindholz

nachrichtlich:
Sekretariat des
Ausschusses für Inneres und Heimat
des Deutschen Bundestages

nur per E-Mail:
Andrea.Lindholz@Bundestag.de
Innenausschuss@Bundestag.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn

FON (0228) 997799-5000
FAX (0228) 997799-5550

E-MAIL referat34@bfdi.bund.de

INTERNET www.bfdi.bund.de

DATUM Bonn, 18.12.2020
GESCHÄFTSZ. 34-681/024#0024

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Gesetzentwurf der Bundesregierung zur Änderung des BND-Gesetzes**

ANLAGEN Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Sehr geehrte Frau Vorsitzende,

der vom Bundeskanzleramt erstellte Gesetzentwurf zur Änderung des BND-Gesetzes (BNDG-E) wurde am 16.12.2020 vom Bundeskabinett beschlossen.

Gegen den BNDG-E bestehen aus meiner Sicht trotz einzelner Verbesserungen, die in den Ressortberatungen erzielt werden konnten, weiterhin erhebliche datenschutzrechtliche Bedenken. Meine fortbestehenden, wesentlichen Kritikpunkte habe ich in der anliegenden Stellungnahme ausgeführt. Ich wäre Ihnen dankbar, wenn Sie den Ausschussmitgliedern meine Stellungnahme für die weitere parlamentarische Beratung zuleiten könnten.

Für etwaige Rückfragen stehe ich dem Ausschuss selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen

[redacted]

Ulrich Kelber

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 18.12.2020

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

an den Ausschuss für Inneres und Heimat des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung zur Änderung des BND-Gesetzes

Der vom Bundeskanzleramt erstellte Gesetzentwurf zur Änderung des BND-Gesetzes (BNDG-E) wurde am 16.12.2020 vom Bundeskabinett beschlossen. Meine Kritikpunkte habe ich in drei Stellungnahmen im Rahmen der Ressortabstimmung vorgetragen. Gegen den BNDG-E bestehen aus meiner Sicht trotz einzelner Verbesserungen in den Ressortberatungen weiterhin die nachfolgenden, wesentlichen Bedenken.

I. Beratung im Ressortkreis

Der Gesetzentwurf wurde seit der ersten Befassung im Ressortkreis Ende September 2020 nach nur drei Monaten in das Kabinett eingebracht. Den engen Zeitplan habe ich wiederholt gegenüber dem Bundeskanzleramt kritisiert. Innerhalb dieses Zeitraums hat das Bundeskanzleramt den Ressorts vier verschiedene, jeweils erheblichen Änderungen unterliegende Entwürfe zugeleitet, für die jeweils nur wenige Tage Zeit zum Kommentieren eingeräumt wurde. Es war ausgeschlossen, das komplexe Regelwerk innerhalb dieser Zeitspanne mit der gebotenen Sorgfalt zu prüfen.

Der enge Zeitrahmen wird der hohen Grundrechtsrelevanz des BNDG-E nicht gerecht. Zur Vermeidung verfassungsrechtlicher Risiken wäre die Einhaltung des Grundsatzes Gründlichkeit vor Schnelligkeit dringend geboten gewesen. Das Vorgehen des Bundeskanzleramtes verstößt in eklatanter Weise gegen die Vorgaben der Gemeinsamen Geschäftsordnung der Bundesministerien. Deutliche Kritik am Zeitplan des Bundeskanzleramtes wurde auch in der Verbändeanhörung geübt.

Eine Folge des Zeitdrucks war, dass keine ausreichende Beratung der während der Ressortbefassung ergangenen Entscheidung des EuGH (Az: C-623/17) in der Rechtssache „Privacy International“ vom 06.10.2020 erfolgte. Der EuGH hat in seiner Entscheidung die EU-Rechtswidrigkeit nationaler Regelungen festgestellt, die Betreiber elektronischer

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Kommunikationsnetze die Pflicht auferlegen, den Sicherheits- und Nachrichtendiensten eines Mitgliedstaats in allgemeiner und unterschiedsloser Weise Verkehrs- und Standortdaten zum Zwecke des Schutzes der nationalen Sicherheit zu übermitteln. Diese Entscheidung hätte im Hinblick auf möglichen Änderungsbedarf des BNDG-E berücksichtigt werden müssen. Dieses Versäumnis sollte im parlamentarischen Verfahren nachgeholt werden.

II. Materiell-rechtliche Bedenken

Die aus meiner Sicht vorrangig verbleibenden materiell-rechtlichen Bedenken möchte ich im Folgenden darstellen, damit diese in die weiteren Beratungen des BNDG-E einfließen können. Auf eine Darstellung sämtlicher von mir in meinen drei Stellungnahmen gegenüber dem Bundeskanzleramt geäußerten Kritikpunkte habe ich verzichtet.

1. Politische Unterrichtung der Landesregierung

Die im dritten Referentenentwurf des BNDG-E vorgesehene Verarbeitung von Daten aus der strategischen Ausland-Fernmeldeaufklärung (A-FMA) zum Zweck der politischen Unterrichtung einer Landesregierung wurde aus der Kabinettfassung des § 19 Abs. 1 Nr. 1 BNDG-E gestrichen, jedoch soll der BND gem. § 29 Abs. 1 Nr. 2 BNDG-E weiterhin an das Bundesamt für Verfassungsschutz, die Verfassungsschutzbehörden der Länder und an den Militärischen Abschirmdienst personenbezogene Daten aus der strategischen A-FMA übermitteln dürfen, welche „*zum Zweck der Unterrichtung […] einer Landesregierung*“ gekennzeichnet sind.

Das Gleiche gilt bei Daten aus dem Eingriff in informationstechnische Systeme mittels sogenannter Computer-Network-Exploitation gem. § 34 Abs. 1 BNDG-E. Die entsprechende Übermittlungsvorschrift sieht gem. § 38 Abs. 1 Nr. 2 BNDG-E ebenfalls die Übermittlung von personenbezogenen Daten „*zum Zweck der Unterrichtung […] einer Landesregierung*“ vor.

Das Bundesverfassungsgericht (BVerfG) hat in seiner Entscheidung (1 BvR 2835/17[1]) vom 19.05.2020 zur strategischen A-FMA ausschließlich die politische Unterrichtung der Bundesregierung in außen- und sicherheitspolitischen Fragestellungen durch den Bundesnachrichtendienst (BND) erlaubt. Die Ergebnisse aus der strategischen A-FMA

[1] Alle nicht anders gekennzeichneten Angaben zu Randnummern beziehen sich auf das Urteil des BVerfG vom 19.05.2020 - 1 BvR 2835/17.

sollen „*allein der Information der Bundesregierung*“ dienen (Rn. 160) und zwar „*auf Regierungsebene*“ (Rn. 226), also der höchsten politischen Entscheidungsebene. Zudem soll die „*Versorgung der Bundesregierung mit Informationen für ihre außen- und sicherheitspolitischen Entscheidungen [helfen] […], sich im machtpolitischen Kräftefeld der internationalen Beziehungen zu behaupten.*“ (Rn. 162). Dies schließt die Landesregierungen nicht mit ein.

Ich empfehle daher, den Zusatz bei den Übermittlungsvorschriften „*[…] einer Landesregierung*“ sowohl in § 29 Abs. 1 Nr. 2 als auch in § 38 Abs. 1 Nr. 2 BNDG-E zu streichen.

2. Privilegierung der Inlandsnachrichtendienste und anderer inländischer öffentlicher Stellen durch Kenntnisnahme von Daten zur politischen Unterrichtung der Bundesregierung

Die in den §§ 29 Abs. 1, 2 und 38 Abs. 1, 2 BNDG-E enthaltenen Übermittlungsvorschriften für Daten aus der strategischen A-FMA bzw. dem Eingriff in informationstechnische Systeme „zum Zweck der politischen Unterrichtung“ sehen zu Unrecht Privilegierungen der Inlandsnachrichtendienste und der anderen inländischen öffentlichen Stellen (inklusive der Polizeien) vor.

Die vom BVerfG vorgesehene Unterscheidung zwischen Daten „zur Gefahrenfrüherkennung“ und von Daten „zur politischen Unterrichtung der Bundesregierung“ und die damit verbundenen unterschiedlichen Anforderungen an die Kriterien (Schwellen) für die Übermittlung dieser Daten an den jeweils zulässigen Adressatenkreis werden durch derartige Übermittlung unterschritten.

Wie dargestellt, sieht das BVerfG ausschließlich die Bundesregierung auf höchster Ebene als Adressat einer Übermittlung von Daten zur politischen Unterrichtung durch den BND an (s. II. 1.). Nach den Vorgaben des Gerichts soll die Bundesregierung beim Rückgriff auf die Daten zur politischen Unterrichtung diese nicht „*an nachgeordnete Behörden im In- und Ausland zu anderen, insbesondere auch operativen Zwecken [weitergeben]*“ (Rn. 226).

Durch die grundsätzlich fehlende Erlaubnis der Bundesregierung, diese Daten aus der strategischen A-FMA an nachgeordnete Behörden weitergeben zu dürfen, darf auch der BND diese Daten nicht an Inlandsnachrichtendienste und andere inländische öffentliche Stellen als „Zwischenempfänger“ bei der politischen Unterrichtung der Bundesregierung weitergeben. Eine solche Einbindung entspricht auch nicht der Stellung des BND als einzigem Auslandsnachrichtendienst des Bundes.

Offen bleibt zudem, auf welchen gesetzlichen Grundlagen eine solche Unterrichtung der Bundesregierung durch diese Stellen als „Zwischenempfänger“ erfolgen können soll. Der

gewählte Umweg dieser Daten lässt daher den Schluss zu, dass vorrangig nicht zur Unterrichtung der Bundesregierung, sondern zur Kenntnisnahme an diese Stellen übermittelt werden soll. Abseits des Weiterverarbeitungsverbots gem. § 29 Abs. 12 BNDG-E könnten von diesen Stellen eigene neue Ansätze zur Erhebung dieser Daten auf Grundlage der Kenntnisnahme generiert werden, obwohl das BVerfG die Daten zur politischen Unterrichtung hierfür nicht vorsieht.

Die in §§ 29 Abs. 1, 2 und 38 Abs. 1, 2 BNDG-E vorgesehene Möglichkeit, dass die Inlandsnachrichtendienste bzw. andere inländische öffentliche Stellen Kenntnis von Daten aus der strategischen A-FMA bzw. dem Eingriff in informationstechnische Systeme erlangen, die allein mit dem Zweck der politischen Unterrichtung der Bundesregierung vom BND erfasst werden, sollte daher im Gesetzentwurf gestrichen werden, da sie nicht den vom BVerfG vorgegebenen Grenzen zur Übermittlung dieser Daten an Stellen außerhalb der Bundesregierung entspricht.

3. Privilegierung der Inlandsnachrichtendienste durch Kenntnisnahme von Daten zur Gefahrenfrüherkennung

Der BNDG-E sieht in §§ 29 Abs. 1 Nr. 1, 38 Abs. 1 Nr. 1 zudem eine Übermittlungsprivilegierung für Daten aus der strategischen A-FMA und des Eingriffs in informationstechnische Systeme zur Gefahrenfrüherkennung an die Inlandsnachrichtendienste vor.

Nach dem BVerfG dürfen personenbezogene Daten aus der strategischen A-FMA nur dann an „andere Stellen“ – was die Inlandsdienste umfasst – übermittelt werden, wenn die Übermittlung durch eine normenklare und hinreichend bestimmte Rechtsgrundlage an den Schutz von Rechtsgütern und an Eingriffsschwellen gebunden wird. Übermittlungen sind danach nur zum Schutz besonders gewichtiger Rechtsgüter gerechtfertigt und setzen als Übermittlungsschwelle eine konkretisierte Gefahrenlage oder, bei Übermittlungen zu Zwecken der Strafverfolgung, einen hinreichend konkretisierten Tatverdacht voraus (Rn. 211).

Entgegen dieser Vorgaben knüpft § 29 Abs. 1 Nr. 1 BNDG-E das Vorliegen tatsächlicher Anhaltspunkte indes nicht an das Vorliegen einer konkretisierten Gefahrenlage für besonders gewichtiger Rechtsgüter an, sondern lediglich an die „Erforderlichkeit“ zum Schutz dieser Rechtsgüter. Hiermit wird die vom BVerfG geforderte Schwelle (Gefahrenkonkretisierung) für Übermittlung von Daten zur Gefahrenfrüherkennung unterlaufen, weshalb die Norm entsprechend unter Einfügung des Kriteriums der „konkretisierten Gefahrenlage“ für besonders gewichtige Rechtsgüter anzupassen ist.

Entsprechendes gilt gem. § 38 Abs. 1 Nr. 1 BNDG-E auch für die Übermittlungen aus dem Eingriff in informationstechnische Systeme, da auch hier ebenfalls lediglich auf die „Erforderlichkeit“ zum Schutz besonders gewichtiger Rechtsgüter statt auf eine konkretisierte Gefahr für diese Rechtsgüter abgestellt wird.

Auch wenn der in § 34 BNDG-E normierte „Eingriff in informationstechnische Systeme von Ausländern im Ausland“ erstmals mit dem gegenständlichen Gesetzentwurf geregelt wird, müssen für diesen, da er aufgrund seines individuellen Charakters eine erheblich größere Eingriffsintensität besitzt, als Maßnahmen der strategischen A-FMA, die vorgenannten Schwellen des BVerfG für Übermittlungen der durch einen solchen Eingriff erlangten Daten an andere inländische Behörden erst recht gelten.

4. Inlandsübermittlungen zur Gefahrenabwehr

§ 29 Abs. 4 BNDG-E bedarf, wie auch die übrigen entsprechend zur Gefahrenabwehr ausgestalteten Übermittlungsvorschriften, zusätzlich noch einer Anpassung durch die Streichung des Wortes „insbesondere“, welches Rechtsunsicherheit durch einen nicht abschließenden Charakter der Übermittlungsvorschriften suggeriert. Die Zusatzregelung in § 29 Abs. 4 Nr. 1 BNDG-E bedarf ebenfalls noch der Streichung, da andernfalls eine Umgehung der Übermittlungsschwellen des § 29 Abs. 4 Nr. 2 BNDG-E droht.

5. Inlandsübermittlungen zur Strafverfolgung

Der im BNDG-E in den Übermittlungsvorschriften gem. §§ 29, 38 BNDG-E enthaltene, nachrichtendienstrechtlich geprägte Begriff der „tatsächlichen Anhaltspunkte“ sollte in Bezug auf Datenübermittlungen an inländische Strafverfolgungsbehörden (§§ 29 Abs. 3, 38 Abs. 3 BNDG-E) durch die vom BVerfG gewählte Formulierung der *„konkreten und in gewissem Umfang verdichteten Umstände als Tatsachenbasis für den Verdacht“* ersetzt werden (Rn. 222).

Ohne entsprechende Änderung im Gesetzestext wird durch die nachrichtendienstrechtlich auszulegende Formulierung der „tatsächlichen Anhaltspunkte“ eine im Verhältnis zu den Vorgaben des BVerfG zu frühzeitige Übermittlung an Strafverfolgungsbehörden ermöglicht, da bei der Auslegung der „tatsächlichen Anhaltspunkte“ auf die nachrichtendienstliche Erfahrungs- und Erwartungshaltung abgestellt wird. Das BVerfG hat aber ausdrücklich klargestellt, dass die Übermittlungsschwelle „wie bei einer Wohnraumdurchsuchung gem. § 100c StPO“ auszugestalten ist (Rn. 222). Damit ist die Übermittlungsschwelle strafprozessual zu verstehen und auszugestalten.

Eine Übermittlung zur Strafverfolgung kann damit erst dann in Betracht kommen, wenn auch die Strafverfolgungsbehörden unter vergleichbaren Umständen, „wie“ etwa bei einer akustischen Wohnraumüberwachung im Sinne des § 100c StPO, an derartige Daten bzw. Erkenntnisse gelangen könnten. Damit soll eine dem Trennungsgebot nicht entsprechende Vorverlagerung des Übermittlungszeitpunkts in den nachrichtendienstrechtlich geprägten Erkenntnisbereich der „tatsächlichen Anhaltspunkte“ vermieden werden.

Ergänzend weise ich darauf hin, dass die § 29 Abs. 3 Nr. 2 BNDG-E aufgeführten §§ 17, 18 AWG noch einer vom BVerfG vorgesehenen Begrenzung auf besonders schwere Straftatbestände bedürfen.

6. Verweis auf Aufgabenerfüllung bei Übermittlungen

Die gesetzliche Formulierung „zur Erfüllung seiner Aufgaben“ wurde vom BVerfG bei der für verfassungswidrig erachteten Übermittlungsvorschrift des § 24 BNDG als unbestimmt angesehen: „Eine allgemeine Bezugnahme auf die gesamten Aufgaben des Bundesnachrichtendienstes […] lässt jedoch nicht erkennen, zu welchen Zwecken hier eine Datenübermittlung erlaubt werden soll“ (Rn. 311, 215). Trotzdem wird im BNDG-E bei den Übermittlungsvorschriften in §§ 29 Abs. 1, 2, 30 Abs. 1, 38 Abs. 1, 2, 39 Abs. 1 BNDG-E weiterhin allgemein auf die Aufgabenerfüllung des BND abgestellt. Dies sollte revidiert und die Aufgaben präzisiert werden.

7. Allgemeine Inlandsübermittlungsvorschriften werden nicht angepasst

Äußerst bedenklich ist, dass die Regelungen des § 24 BNDG nicht angepasst und in § 11 BNDG-E unverändert fortbestehen. Dabei wurde § 24 BNDG vom BVerfG auch aus anderen Gründen, abseits der verfassungsrechtlichen Vorgaben zur strategischen A-FMA, für verfassungswidrig erachtet (Rn. 311 ff.). Der BNDG-E sieht damit in bemerkenswerter Weise die Aufrechterhaltung dieser Regelungen vor, obwohl das BVerfG dem Gesetzgeber eine Neuregelung bis zum Ablauf der Fortgeltungsanordnung spätestens zum 31. Dezember 2021 auferlegt hat. Als praktische Folge der Nichtanpassung wird der BND nach Ablauf der Fortgeltungsanordnung insoweit keine allgemeinen Übermittlungen mehr vornehmen können.

8. Verkehrsdatum/Metadatum; Recht auf informationelle Selbstbestimmung

In § 26 BNDG werden ohne Legaldefinition „Verkehrsdaten“ und „personenbezogene Verkehrsdaten“ aufgeführt, während in der Gesetzesbegründung ergänzend „personenbezogene Metadaten“ und „sonstigen Metadaten“ „neben Verkehrsdaten“ genannt werden (Begründung S. 85 ff.). Infolge fehlender Legaldefinitionen wird in § 26 BNDG-E eine Be-

stimmtheit des Begriffs der (personenbezogenen) Verkehrsdaten suggeriert, die nicht vorhanden ist. Es kommt hierdurch zu Unklarheiten, ab welcher Schwelle eine Abgrenzung zu den Inhaltsdaten der Kommunikation erfolgt. Die Begriffsunklarheit führt so auch zu Folgeproblemen beim Schutz vom BND erhobener Verkehrsdaten von inländischen Grundrechtsträgern. Faktisch wird in sehr vielen Fällen der zunächst erteilte Schutz der Verkehrsdaten von § 26 Abs. 3 S. 2 BNDG-E bei Daten der Maschine-zu-Maschine-Kommunikation wieder aufgehoben. Mit der Maschine-zu-Maschine-Kommunikation ist die Kommunikation eines personalisierten Endgeräts gemeint, welche keinen menschlichen Kommunikationspartner hat.

In der Gesetzesbegründung wird diese Kommunikationsform in bagatellisierender Weise als „bloße Maschine-zu-Maschine-Kommunikation“ bezeichnet (Begründung S. 86). Es wird damit das Bestehen einer unwichtigen Kommunikationsform suggeriert, obwohl diese die meistgenutzte Kommunikationsform der Zukunft mit dem „internet of things“ als Teilaspekt des dort zu erwartenden Kommunikationsumfangs sein dürfte. Tatsächlich sind in jedem Endgerät (z.B. Synchronisation eines Smartphones) große Anteile von Maschinenkommunikation enthalten. Dabei generiert die Maschine-zu-Maschine-Kommunikation mitunter private und tiefer eingreifende und umfassendere Erkenntnismöglichkeiten als diese durch eine Telefonüberwachung generiert werden können, selbst wenn die Kommunikation nicht von einem Menschen ausgelöst wurde.

§ 26 Abs. 3 S. 3 BNDG-E sieht zusätzlich die Möglichkeit vor, dass diese Verkehrsdaten zur Erfüllung der Aufgaben des BND weiterverarbeitet werden dürfen, wenn diese im Sinne des Gesetzes unkenntlich gemacht werden. Das Bundesverwaltungsgericht (BVerwG) hat im VERAS-Urteil bereits die Praxis des BND der Unkenntlichmachung der Verkehrsdaten bei Grundrechtsträgern für nicht hinreichend erklärt, weil über Koinzidenz des Kommunikationszeitpunkts/-zeitraums und des Kommunikationsorts eine Repersonalisierung möglich sei (BVerwG 6 A 6.16, Rn. 26). Das wird im BNDG-E nicht geändert und sogar erleichtert.

Durch einfache Koinzidenzbetrachtung kann vom BND weiterhin zwischen den ungeschützten Daten gem. § 26 Abs. 3 S. 2 Nr. 1 BNDG-E und den unkenntlich gemachten Daten gem. § 26 Abs. 3 S. 2 Nr. 2 BNDG-E auf die Person zurückgeschlossen werden bzw. die personenbeziehbaren Daten ermittelt werden. Die Zuweisung erfolgt über eine scheinbar zufällige aber doch konstante Kennung „desselben Telekommunikationsmerkmals“ durch „immer denselben Hashwert“ (Begründung S. 88). Folglich ist von einer aufhebbaren Pseudonymisierung auszugehen, da der BND den Personenbezug mit eigenen Daten über einen schlichten Datenvergleich wiederherstellen kann.

Aus den vorgenannten Gründen sollten Legaldefinitionen eingeführt werden. Die Pseudonymisierung muss durch eine Anonymisierung ersetzt werden, um einer umfangreichen Überwachung von inländischen Grundrechtsträgern zu begegnen, welche besonderen verfassungsrechtlichen Risiken ausgesetzt ist.

9. Überwachtes Internetaufkommen

Die Beschränkung des überwachten Internetverkehrsaufkommens aus den undefiniert gelassenen „bestehenden Telekommunikationsnetzen“ bedarf der Überarbeitung. Zwar wurde die prozentuale Grenze von 50% auf nominal 30% gem. § 19 Abs. 8 BNDG-E verringert. Dies führt jedoch zu keiner vom BVerfG geforderten tatsächlichen Beschränkung. Die Gesetzesbegründung erklärt den an sich unscharfen Begriff der „bestehenden Telekommunikationsnetze“ mit der Kapazität aller weltweiten Telekommunikationsnetze und nicht mit der effektiv genutzten Datenrate der für den BND praktisch erreichbaren und überwachbaren Telekommunikationsnetze. Insofern muss beachtet werden, dass ein erheblicher Teil der Kapazität von geschätzten 50% im jeweiligen Netz etwa zur Abfederung von Lastspitzen vorgehalten werden. Damit nimmt die nominale Beschränkung auf die unrealistisch hohe Gesamtkapazität sämtlicher weltweit bestehender Telekommunikationsnetze Bezug. So können die vom BND erreichbaren und überwachbaren Telekommunikationsnetze mit denen, die praktisch außerhalb seines Zugriffs sind, verrechnet werden. Die prozentuale Grenze von 30% der weltweiten Netzkapazität dürfte eher einer 100%igen-Überwachungserlaubnis der effektiven Datenströme in den erreichbaren Telekommunikationsnetzen entsprechen.

Um auch hier verfassungsrechtlichen Risiken zu begegnen, sollte im Gesetz die Beschränkung auf eine taugliche Bezugsgröße erfolgen. Die Verwendung effektiver Datenraten auf den dem BND zur Verfügung stehenden Übertragungswegen anstelle von Datenkapazitäten würde beispielsweise in die richtige Richtung führen.

10. Eingriff in informationstechnische Systeme / Quellen-TKÜ

Die §§ 34, 38 BNDG-E beinhalten gesetzlich neue, besonders intensive Grundrechtseingriffe durch den Eingriff in informationstechnische Systeme / Computer-Network-Exploitation samt der Ermächtigung zur Durchführung einer Quellen-TKÜ und den daraus folgenden Inlandsübermittlungen.

Die Erhebungsschwellen zur politischen Unterrichtung gem. § 34 Abs. 2 BNDG-E und zur Gefahrenfrüherkennung gem. § 34 Abs. 3 BNDG-E sind verfassungsrechtlichen Risiken ausgesetzt. Es empfiehlt sich jedenfalls für die Gefahrenfrüherkennung trotz des Auslandsbe-

zuges eine Anhebung der Erhebungsschwelle mindestens annähernd auf das Niveau der Schwellenvorgabe, welche im Urteil des BVerfG zur Onlinedurchsuchung (BVerfG 1 BvR 966/09, Rn. 212) festgesetzt wurde. In dieser Entscheidung wurde ohne Auslandsbezug für den zielgerichteten Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme das Erfordernis von „*tatsächlichen Anhaltspunkten für eine im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut*“ gefordert (BVerfG 1 BvR 966/09, Rn. 212). Auf dieses Urteil hat das BVerfG im Urteil zur strategischen A-FMA ausdrücklich Bezug genommen, indem es klargestellt hat, dass das Urteil zur Onlinedurchsuchung auch für die Nachrichtendienste Geltung entfaltet (Rn. 141).

Auch die Übermittlungsvorschrift gem. § 38 BNDG-E sehe ich verfassungsrechtlichen Risiken ausgesetzt. In der Gesetzesbegründung wird zwar ausgeführt, dass die Übermittlung gem. § 38 BNDG-E auch gegenüber den bereits erhöhten Schwellen der §§ 29 ff. BNDG-E ein eigenes Übermittlungsregime erfordert, das der Eingriffsschwere vor dem Hintergrund des Verhältnismäßigkeitsgrundsatzes Rechnung trägt (Begründung S. 114). Hinter diesem Anspruch bleibt aber insbesondere § 38 BNDG-E zurück, welcher lediglich bei der Übermittlung zur Strafverfolgung „Tatsachen, die die Annahme rechtfertigen“ anstatt „tatsächlicher Anhaltspunkte“ im Vergleich zu § 29 BNDG-E als leicht stärker ausgestaltete Übermittlungsschwelle vorsieht.

Im Übrigen ist es dringend notwendig, dass das „informationstechnische System“ als eine zentrale Begrifflichkeit nicht nur im BNDG-E eine gesetzliche Definition erfährt.

11. Kooperation der Kontrollorgane

Die Kooperationsregelung gem. § 58 Abs. 2 BNDG-E zwischen den Kontrollorganen bedarf der Nachbesserung. Mir ist nach dieser Regelung keine inhaltliche Kooperation mit den anderen Kontrollorganen möglich.

Ein Austausch lediglich über „allgemeine Angelegenheiten“ der Kontrolltätigkeit, wie in § 58 Abs. 2 BNDG-E vorgesehen, ist unzureichend. Selbstverständlich muss zwischen den Kontrollorganen ein inhaltlicher Austausch möglich sein, um Kontrolllücken bzw. „Doppelkontrollen“ vermeiden zu können. Durch die Vorgabe eines Austausches nur über „allgemeine Angelegenheiten“ werden die Effektivität und Synergien bei Kontrollen erschwert.

Im Übrigen sollte die Überschrift des § 58 BNDG-E noch angepasst werden. Es muss heißen: „Zusammenarbeit zwischen dem Unabhängigen Kontrollrat […]“.

12. Fragliche Distanz des Unabhängigen Kontrollrats zum BND

Die vom BVerfG geforderte notwendige Distanz des Unabhängigen Kontrollrats zum BND könnte durch die gesetzlich geregelten Einflussmöglichkeiten des Bundeskanzleramtes beeinträchtigt werden.

Gem. § 41 Abs. 5 BNDG-E ist das Bundeskanzleramt vor Erlass einer Geschäftsordnung und Verfahrensordnung des unabhängigen Kontrollrats anzuhören. Gem. § 41 Abs. 1 BNDG-E sind als Dienstsitze Berlin und Pullach vorgesehen. Unklar bleibt dabei, ob der Unabhängige Kontrollrat auf den Liegenschaften des BND den Dienstsitz oder Büros annehmen soll und so die notwendige Distanz faktisch unterlaufen wird. Gem. § 55 Abs. 3 BNDG-E ist das Bundeskanzleramt vor Veröffentlichung einer abstrakten Unterrichtung des Bundestages zunächst anzuhören. Gem. § 57 Abs. 2 BNDG-E darf der unabhängige Kontrollrat dem Bundeskanzleramt und damit der dem BND übergeordneten Behörde die Personalverwaltung und Personalwirtschaft übertragen. Schon aufgrund der Herausforderung, die gerichtsähnliche Kontrolle von Grund auf in kürzester Zeit aufbauen zu müssen, ist davon auszugehen, dass dem unabhängigen Kontrollrat keine andere Wahl bleiben wird, als dieses Angebot anzunehmen. Von besonderer Bedeutung ist dies deshalb, weil das BVerfG im Urteil bereits „*auf eine ausgewogene Zusammensetzung der Kontrollinstanzen*“ wert gelegt hat, bei welcher „*zur Sicherstellung der gebotenen Unabhängigkeit auf die Wahrung einer hinreichenden Distanz zum Bundesnachrichtendienst*“ zu achten ist (Rn. 287).

In der gegenwärtigen Fassung des BNDG-E erscheint die erforderliche Distanz noch nicht hinreichend abgesichert, weshalb der Gesetzentwurf insoweit nachgebessert werden sollte.

13. Fehlende Anordnungsbefugnis des BfDI

Der BfDI kann auch nach dem aktuellen BNDG-E weiterhin lediglich Beanstandungen aussprechen, die bereits durch die Äußerung einer gegenteiligen Rechtsauffassung unberücksichtigt bleiben können. Im Sinne einer wirksamen Kontrolle sollte der BfDI entsprechend § 69 Abs. 2 BKAG konkrete Anordnungsbefugnisse gegenüber dem BND bei festgestellten Datenschutzverstößen erhalten.

14. Übergangsregelungen

Der Wortlaut des § 69 Abs. 1 S. 2 BNDG-E ist missverständlich gewählt und bedarf der klarstellenden Aufnahme des BfDI im Hinblick auf die mir zustehenden Kontrollrechte, da der Wortlaut die Rechtskontrolle ausschließlich durch die administrative Kontrolle vorsieht.