VERBAND DER INTERNETWIRTSCHAFT E.V.

eco Stellungnahme zum RefE eines Gesetzes zur Änderung des Gesetzes über den Bundesnachrichtendienst zur Umsetzung der Vorgaben aus dem Urteil des Bundesverfassungsgerichts vom 19. Mai 2020 (1 BvR 2835/17)

Berlin, 3. Dezember 2020

Das Bundeskanzleramt hat am 25.11.2020 einen Entwurf des BND-Gesetzes bekannt gegeben und zur Konsultation gestellt. Anlass zur Änderung geben die Urteile des Bundesverfassungsgerichts, 1 BvR 2835/17 und Urteile des Bundesverwaltungsgerichts, 6 A 6.16 u 6 A 7.16. Der Entwurf soll noch dieses Jahr im Bundeskabinett beschlossen werden. Es besteht daher gesetzgeberischer Handlungsbedarf, da die verfassungswidrigen Regelungen im BND-Gesetz längstens bis 31.12.2021 weiter angewendet dürfen. Der Gesetzgeber will mit den Änderungen den gerichtlichen Vorgaben der genannten Urteile Rechnung tragen.

Diesem Ziel wird der Entwurf nur unzureichend gerecht. Dies gilt unter anderem für technische Kontrolle der Aufklärung durch den BND und für die administrative Rechtskontrolle. Darüber hinaus werden Vorgaben des Gerichts teilweise missachtet. eco sieht hier dringenden Nachbesserungsbedarf.

Aufgrund der kurz bemessen Anhörungsfrist beschränken wir uns auf die wichtigsten Aspekte. Weitere Anmerkungen wird eco im weiteren Verlauf des Gesetzgebungsverfahrens einbringen.

I. Anhörungsdauer unangemessen

Die Frist der Verbändebeteiligung ist mit einer Woche deutlich zu kurz bemessen. Dies ist weder der Eingriffsintensivität noch der Vielzahl der Betroffenen noch dem Umfang und der Bedeutung des Gesetzgebungsverfahrens angemessen.

II. Aufhebung des Personenbezugs (§ 2 BNDG-E i. V. m. den § 10 bis § 18 BNDG-E)

§ 2 Abs. 1 BNDG regelt die allgemeine Befugnis des BND, Informationen einschließlich personenbezogener Daten zu verarbeiten. Indem der Gesetzgeber vorschlägt, in den §§ 10 bis 18 BNDG-E[1] das Wort „Informationen“ zu streichen, wären diese Normen mit ihren tatbestandlichen Einschränkungen nur noch auf personenbezogene Daten anwendbar. Daraus folgt, dass Daten ohne Personenbezug nach § 2 BNDG verarbeitet werden dürfen.

[1] Paragraphen ohne weitere Bezeichnung im Folgenden beziehen sich auf das BNDG-E im Artikel 1 des Referentenentwurfs.

Das führt nach Ansicht des eco zu drei Problemfeldern:

- Kaum Schranken bei Ausnahmen, die eine immense Vielzahl von Lebenssachverhalten erfassen, so dass mitnichten von einer Ausnahme gesprochen werden kann (vgl. § 26 Abs. 3 S. 2 u. S. 3),

- Ebenso wenig bestehen Schranken bei untauglichen Mitteln zur Entfernung des Personenbezugs (vgl. § 26 Abs. 2 S. 3),

- Kaum Schranken bei Erfassung und Verarbeitung, falls der BND seine Auslegung und Interpretation durchsetzen kann, es handele sich bei „nicht menschlicher Kommunikation“ nicht um personenbezogene Daten.

Die ersten zwei genannten Problemfelder werden die zuletzt genannte Problematik in ihrer Relevanz erheblich steigern. Bei einer kaum vorhandenen Einordung und Anerkennung des Vorliegens von einem Personenbezug von Daten, gibt es kaum Einschränkungen bei der Verarbeitung. Die Regelung in § 2 BNDG enthält im Vergleich zu den Normen mit dem Tatbestandsmerkmal „personenbezogenen Daten“ (§§ 19, 26) deutlich weniger Schranken für die Aufklärungstätigkeit des BND.

eco erachtet ein vom Gesetzgeber beabsichtigtes Auflösen des Personenbezugs weder als sachgerecht noch angemessen. Vielmehr handelt es um einen Kunstgriff, wodurch der BND möglichst wenig Schranken unterliegen soll. Das ist nicht akzeptabel.

Weitergehende Ausführungen zu § 26 Absatz 3 finden sich unter V.

III. Kritik an strategischer Ausland-Fernmeldeaufklärung (§ 19)

Nahezu schrankenloser Zugriff auf andere als Inhaltsdaten nach 19 Abs. 1

Nach dem Tatbestand soll sich die Vorschrift auf die Befugnis des BND zum Zweck der strategischen Ausland-Fernmeldeaufklärung mit technischen Mitteln auf die Verarbeitung personenbezogener Inhaltsdaten beziehen. Die Beschränkungen dieser Ermächtigung nach den Absätzen 2 bis 5 gelten demnach auch nur für personenbezogene Inhaltsdaten. Demzufolge dürften allen andere Arten von Daten gem. § 2 BNDG mit technischen Mitteln verarbeitet bzw. erhoben werden und unterlägen keinen vergleichbaren Beschränkungen wie nach den Absätzen 2 bis 5 des § 19. eco lehnt eine derartige Ermächtigung entschieden ab. Nach Ansicht des eco stellt dies einen Verzicht auf konkretisierende Eingriffsschwelle dar und kommt einer Freistellung von einem Kernelement rechtsstaatlicher Anforderungen gleich. Dieses Kernelement ist jedoch grundsätzlich und insbesondere in Bezug auf innerstaatlich tätige Sicherheitsbehörden schon für weniger intensive Grundrechtseingriffe wie die Verkehrsdatenerhebung unverzichtbar.[2]

[2] Vgl. 1 BvR 2835/17, Rn. 155.

Definition von Suchbegriffen nach § 19 Abs. 5

Der Begründung zu §19 Abs. 5 (S. 67) ist nunmehr offensichtlich zu entnehmen, dass das konventionelle Verständnis von Suchbegriffen, wie es zumeist auch im Rahmen der gerichtlichen Verfahren verwendet wird, nicht der Praxis in den Filtersystemen des BND entspricht.

eco hat bereits mehrfach, so auch im Rahmen des Verfahrens vor dem BVerfG, darauf hingewiesen, das sogenannte reguläre Ausdrücke, Hashwerte oder gar binäre Suchparameter bestenfalls mit einem hohen Aufwand oder im Fall von binären Suchparametern ggf. überhaupt nicht auf deren konkrete Wirkung in der Filterung von Kommunikationsverkehren geprüft werden können und insofern erhöhte Anforderungen an derartige Suchbegriffe gestellt werden müssen.

Beispielsweise kann eine Prüfung derartiger Suchbegriffe im Rahmen der administrativen Kontrolle daher ausschließlich anhand statistischer Parameter zu dem jeweiligen Suchbegriff (z.B. konkrete Trefferzahl, Anzahl der Treffer je Anzahl Verkehre) bewertet werden und erfordert insbesondere neben der positiven auch eine negative Abschätzung der Wirkung des individuellen Suchbegriffes (z.B. unspezifische oder überbordende Anzahl von Treffern durch den jeweiligen Suchbegriff).

Staatliches Eindringen (Hacking) nach § 19 Abs. 6

Der Entwurf beinhaltet in § 19 Abs. 6 (sowie § 26 Abs. 1) eine Erlaubnis für den BND, Anbieter im Ausland hacken zu dürfen um sowohl Bestand-, Verkehrs- als auch Inhaltsdaten ohne Wissen des jeweiligen Betreibers zu erlangen. Auffällig ist aus Sicht des eco, das offenbar bewusst in Kauf genommen wird das von den im vorliegenden Entwurf vorgesehen Regelungen bspw. auch Plattformbetreiber wie Google, Facebook, Amazon und Apple betroffen wären, grundsätzlich sind darüber hinaus aber alle TK-Dienstanbieter, alle Clouddienste und auch alle weiteren Anbieter von Telemediendiensten im Ausland als potentielle Ziele eines staatlichen Eindringens betroffen. Daher sind von einer solchen Ermächtigung auch die Mehrzahl der Bundesbürger, welche in der Regel die genannten Dienste nutzen, betroffen.

Dieser Ansatz bildet einen massiven Anreiz für staatliche Akteure, Dienste und berechtigte Stellen sich Softwarelücken in weitverbreiteten Anwendungen und System zu beschaffen und diese geheim zu halten. Dies schwächt nicht nur die IT-Sicherheit und die Integrität von IT-Infrastrukturen, sondern auch allgemein die Vertrauenswürdigkeit von Kommunikation und das Vertrauen in digitale Dienste.

Zudem stellt ein solches Vorgehen die Bundesrepublik Deutschland in den Konflikt mit anderen Staaten und gleichzeitig den Grundrechten der Bürger, da damit ein Eingriff in das Recht auf informationelle Selbstbestimmung sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einhergeht.

Die mit dem Entwurf vorgeschlagene Regelung bzw. diese Ermächtigung erinnert insofern stark an entsprechende Regelungen anderer Länder, welche von Deutschen Sicherheitspolitikern im Laufe des letzten Jahres als nicht mit den deutschen Sicherheitsinteressen vereinbar kritisiert wurden und im Rahmen von Diskussionen über potentielle Ausschlüsse von Anbietern einen breiten Raum in der öffentlichen Diskussion eingenommen hat.

Automatische Filtersysteme nach § 19 Abs. 7

Die Vorgabe des Bundesverfassungsgerichts, dass die eingesetzten Filtersysteme zur Einhegung unzulässiger Überwachung dem Stand der Wissenschaft und Technik entsprechen müssen, vgl. Rn. 173 v. 1 BvR 2835/17, wird in dem Gesetzentwurf nicht berücksichtigt. Gem. § 19 Abs. 7 S. 4 wird allein der „Stand der Technik“ als ausreichend erachtet. Dies stellt eine deutlich geringere Anforderung dar. Das BVerfG hat bewusst die höchste Anforderung gesetzt, wie sie beispielsweise im Atomgesetz vorgesehen und geregelt ist. Nach Ansicht des eco stellt dies einen eklatanten Verfassungsbruch dar. Die im Entwurf vorgesehene deutliche geringere Anforderung „Stand der Technik“ hätte praktisch zur Folge, dass der BND von Gesetzes wegen nicht verpflichtet wäre, selbstlernende, auf künstlicher Intelligenz basierte Filter einzusetzen, wie sie heute bereits im industriellen Umfeld eingesetzt werden. Der Einsatz solcher Filtersysteme würde aber dem aktuellen „Stand der Wissenschaft und Technik“ entsprechen und sollte dementsprechend als gesetzliche Anforderung an die eingesetzten Filtersysteme vorgesehen werden.

Selbstrechtfertigende Gefahrenlagen

eco hält es für dringend geboten, dass in des § 19 Abs. 7 Satz 6 eine tatbestandliche Einschränkung vorgenommen und damit klargestellt ist, dass die tatsächlichen Anhaltspunkte für Gefahren nicht den nach Abs. 1 i. V. m. Abs. 7 S. 1 erhobenen Daten selbst entstammen dürfen. Anderenfalls würde alle in Absatz 7 vorgesehenen beschränkenden Tatbestandsmerkmale obsolet und keinerlei Wirkung entfalten.

Änderung/Anpassung der Erfassungsgrenzen nach §19 Abs. 8

eco erkennt an das mit der Reduzierung der Erfassungsgrenzen in § 19 Abs. 8 auf nunmehr 30% Prozent des globalen Verkehrs statt der 50% im bisherigen Entwurf der Versuch unternommen wird, überhaupt eine Begrenzung der Erfassung von Verkehren zu etablieren. Allerdings stellt auch die vorgesehene Anpassung der Erfassungsgrenze auf 30% der Datenverkehre aller weltweiten Telekommunikationsnetze faktisch keine taugliche Begrenzung dar. Zum Vergleich: In §10 Abs. 4 des G10-Gesetzes wird eine Grenze von 20% der dort gegenständlichen Inlands-Auslands-Datenverkehre der Übertragungswege einer einzigen Anordnung gewählt. Diese Verkehre stellen jedoch nur einen kleinen Teil der

Datenverkehre der Bundesrepublik dar, welche wiederum nur einen kleinen Teil der weltweiten Verkehre (ca. 5-7%) generiert. Eine Erfassungsgrenze von 30% der Verkehre aller bestehenden weltweiten Telekommunikationsnetze entspricht deshalb einem Vielfachen der vollständigen Kommunikationsdaten der Bundesrepublik Deutschland - die vorgesehene Erfassungsgrenze entfaltet somit keine tatsächliche Begrenzungswirkung.

Keine Kennzeichnung bei Übermittlungen § 19 Abs. 10 S. 2

Nach Auffassung des eco laufen die Regelungen zur Kennzeichnung von personenbezogenen Daten bei Übermittlungen des BND an andere Stellen weitgehend leer. Denn § 19 Abs. 10 S. 2 ordnet an, dass bei Übermittlungen die Kennzeichnung dieser Daten mit Angabe des Zwecks der Datenerhebung nach § 19 Abs. 1 und Angabe des Mittels der Datenerhebung vollständig entfällt. Nach Ansicht des eco führt das zu, dass die Stellen, denen der BND Daten übermittelt, nicht in der Lage sein werden die Regeln zum Schutz personenbezogener Daten einzuhalten, da diese Stellen mangels Kennzeichnung keine Kenntnis vom Personenbezug haben können.

IV. Kontrollmöglichkeit nicht ausreichend (§ 23 Abs. 5 bis 7)

eco ist der Auffassung, dass die Regelung des § 23 Abs. 6 S. 2 der Wahrnehmung einer wirksamen Kontrolle durch den unabhängigen Kontrollrat entgegensteht. Danach ist in der schriftlichen Anordnung die Nennung einzelner Suchbegriffe, die zur gezielten Datenerhebung verwendet werden, nicht erforderlich. Wenn die Suchbegriffe aber nicht in Anordnung genannt werden oder anderweitig geregelt ist, dass nur temporär verwendete Suchbegriffe einer Maßnahme stets dauerhaft zu speichern sind, ist keine effektive Kontrolle gewährleistet. Nach Auffassung des eco ist der potentielle Umfang einer gezielten Maßnahme nicht prüfbar, ohne dass konkrete Suchbegriffe/Kennungen einer Filterung festgehalten werden, denn erst aus diesen ergibt sich die Zielgenauigkeit der Maßnahme. Eine entsprechende Regelung nur in Dienstvorschriften im Sinne von § 62 hält eco nicht für ausreichend.

V. Dauerhafte und unkontrollierte Eignungsprüfung (§ 24)

Die Vorschriften zur Eignungsprüfung in § 24 wurden bereits in der Vergangenheit durch eco als Einfallstor für eine nahezu beliebige Überwachung von Übertragungswegen kritisiert, welche weder Filtersysteme oder Suchbegriffe erfordert noch einer Kontrolle durch eines der bestehenden Kontrollgremien unterliegen würde. Im vorliegenden Entwurf wurden die bestehenden gesetzlichen Regelungen nicht nur beibehalten, sondern durch Regelungen zur nahezu beliebigen Datenspeicherung verschlüsselter Daten (§ 24 Abs. 1) sowie einer zeitlichen und administrativen Öffnungsklausel versehen, welche sowohl eine permanente Eignungsprüfung als dauerhaftes Instrument ermöglicht (§ 24 Abs. 2 S. 3 „mehrmalige

Verlängerung“) als auch von der Benennung eines konkreten Telekommunikationsnetzes zur Erhebung der Daten absieht (S. 78 RefE, Begründung zu § 24 Abs. 3).

Trotz umfassender Neuregelung und massiver Kapazitätserweiterung der Kontrolle soll das überbordende Instrument der Eignungsprüfung jedoch weiterhin keinerlei Kontrolle durch die Kontrollorgane unterliegen.

eco regt an dieser Stelle an, das Instrument der Eignungsprüfung analog zu anderen Maßnahmen einer Genehmigung durch den Kontrollrat zu unterwerfen.

VI. Aufhebung des Personenbezugs bei Verkehrsdaten (§ 26)

Fehlende Kennzeichnung personenbezogener Daten nach § 26 Abs. 2

Die Regelung in § 26 Abs. 2 sieht in ausdrücklicher Abweichung von § 19 Abs. 10 vor, dass zunächst keine unmittelbare Kennzeichnung der personenbezogenen Daten erfolgt. Das hat zur Folge, dass alle Verkehrsdaten trotz des darin unzweifelhaft enthaltenen Personenbezugs zunächst ohne Kennzeichnung von Quelle oder Anordnungsgrundlage gespeichert werden. Eine entsprechende Kennzeichnung der Daten erst im weiteren Verlauf ist jedoch bereits offensichtlich unmöglich. Ohne sofortige Kennzeichnung ist die Quelle von Daten unbekannt, es könnten im Nachgang bestenfalls Mutmaßungen über beispielsweise deren Verknüpfung zu im Inland auf Basis des G10-Gesetzes erhobenen Daten angestellt werden. Zudem ist eine manuelle Verarbeitung von Verkehrsdaten wie sie in § 26 Abs. 2 vorgesehen ist untypisch und auch aufgrund der Datenmenge kaum durchführbar. Entgegen der gesetzgeberischen Annahme wird hier typischerweise von einer automatisierten Verarbeitung auszugehen sein.

Die vorgeschlagene Regelung werden in der Konsequenz dazu führen, dass sämtliche Vorgänge der automatisierten Verarbeitung wie die Filterung gegen konkrete Suchkriterien, die Erstellung und Profilbildung von Beziehungsnetzwerken oder die Weitergabe von Verkehrsdaten insofern ohne eine Berücksichtigung der Erhebungsgrundlage oder einer konkreten Anordnung erfolgen würde und sich hierdurch einer effektiven Kontrolle in weiten Teilen entzieht.

Aufhebung des Personenbezugs durch Anonymisierung von Verkehrsdaten aus In- und Auslandkommunikation nach § 26 Abs. 3

Die in § 26 Abs. 3 S. 2 Nr. 2 vorgenommene besondere Ermächtigung zur Speicherung und Verarbeitung von „anonymisierten“ Verkehrsdaten aus In- und Auslandskommunikation ist zu hinterfragen, weil die weiteren Kommunikationsteilnehmer und die „Eindeutigkeit der Daten“ im Zuge der Anonymisierung erhalten bleiben sollen. Ein solches Vorgehen ist jedoch dysfunktional. Aufgrund der Natur von Verkehrsdaten ist eine Anonymisierung wie in § 26 Abs. 3 S. 3 vorgesehen in technischer Hinsicht unmöglich, solange auch nur ein

Kommunikationsteilnehmer und ein weiteres eindeutiges Merkmal der Kommunikation bekannt sind. In einer solchen Konstellation ist eine derartige Anonymisierung jederzeit und ohne großen Aufwand durch Korrelation mit Verkehrsdaten einer der Anbieters des A- oder B-Endes der Kommunikation oder auch der Verkehrsdaten anderer Partnerdienste auch im Nachhinein aufhebbar.

Weitere gravierende Bedenken und Zweifel an der Tauglichkeit dieser Regelung werden durch die in der Gesetzesbegründung beschrieben „Verhashung" der Daten als Methode zur vorgeblichen „Anonymisierung" begründet, welche bei Einsatz der beschriebenen Vorgehensweise faktisch sowohl beliebige Kommunikationen einer Person weiterhin zusammenfassbar gestalten als auch den Aufbau einer festen Zuordnungstabelle „Hashwert zu Kennung" ermöglichen, welche bei De-Anonymisierung auch nur einer einzelnen Kommunikation eine Re-Identifizierung aller Kommunikationsvorgänge dieser Person ermöglicht.

Faktisch stellt diese Regelung eine Umgehung des Erfordernisses einer G10-Anordung zur Verarbeitung personenbezogener Verkehrsdaten von Deutschen, inländischen juristischen Personen und sich im Bundesgebiet aufhaltender Personen dar, ohne diesen einen Schutz durch effektive Anonymisierung zu gewährleisten.

Erhebung von maschinell erzeugten Daten im In- und Ausland nach § 26 Abs. 3

Die in dem Gesetzentwurf vorgesehenen Regelungen des § 26 Abs. 3 Satz 3 ermächtigen den BND, personenbezogene Daten auch von Bundesbürgern, inländischen juristischen Personen und sich im Bundesgebiet aufhaltenden Personen jederzeit im In- und Ausland in allen Fällen zu erheben, in denen diese nicht als „menschliche Kommunikation" eingestuft wird. Nach Ansicht des BND umfasst der Schutzbereich des Art 10 GG nur „menschliche Kommunikation". Demzufolge würden alle weiteren Kommunikationen aus Sicht des BND auch bei eindeutigem Personenbezug keinem grundgesetzlichen Schutz unterliegen.

Hierbei ist zu berücksichtigen, dass in vielen Lebenssachverhalten heute ein automatisierter Informationsaustausch stattfindet, unabhängig davon ob es sich dabei beispielsweise um die Informationsbeschaffung im Internet, Online-Banking und Zahlungen, Hotelbuchungen, Navigationssysteme oder die GPS- und Bewegungsdaten von Mobilfunkgeräten handelt.

Nach Einschätzung des eco würde die in dem Gesetzentwurf vorgesehen Regelung und Anwendung dieser gesetzlichen Ermächtigung zukünftig eine umfassende Überwachung des Kommunikationsverhaltens nebst Bewegungsprofilen, Finanztransaktions- und Bewegungsdaten von Personen im In- und Ausland ermöglichen.

Im Ergebnis bleibt festzustellen, dass nach dem vorliegenden Gesetzentwurf dem BND hinsichtlich personenbezogener Verkehrsdaten keine praktisch wirksamen Grenzen oder Beschränkungen bezüglich einer Erhebung, Speicherung und Weiterverarbeitung von

Verkehrsdaten gesetzt werden. Denn die Regelungen von § 26 Absatz 3 S. 2 Nr. 1 führt dazu, dass es für den BND nahezu keine personenbezogenen Daten gibt. Die vorgeschlagene Regelung liest sich zwar wie eine Ausnahme, erfasst aber de facto unendlich viele Lebenssachverhalte (fast alle Internetnutzungen, wie Surfen, Online-Banking, Karten- und Navigationsanwendungen, Mobilfunkbasisstationen-Datensätze, Hotelbuchungen usw.). Denn ab der ersten Veranlassung durch einen Menschen, bspw. der Aufruf einer Homepage oder das Wählen einer (Ruf-)Nummer erfolgt alles weitere automatisch. Falls ausnahmsweise dennoch ein Personenbezug vorhanden und vom Gesetzgeber anerkannt wird (§ 26 Absatz 3 S. 2 Nr. 2 i. V. m. S. 3), wird ein untaugliches Mittel zur Anonymisierung der Daten vorgeschlagen, so dass die Herstellung des Personenbezugs jederzeit und mit geringem Aufwand wieder herstellbar ist.

VII. Hacking gefährdet IT-Sicherheit und schwächt Vertrauenswürdigkeit (§ 34)

eco nimmt Bezug auf die Ausführungen zu § 19 Abs. 6, da die Kritik gleichsam für das Eindringen in IT-Systeme einzelner Personen gilt. Den maximal zulässigen Zeitraum nach § 34 Abs. 7 S. 2 von drei Jahren für eine Prüfung, ob die erhobenen Daten erforderlich sind, erachtet eco als unangemessen lange.

VIII. Regelung der Administrativen Rechtskontrolle unzureichend (§§ 50, 51)

Nach Ansicht des eco sollte in § 50 klargestellt werden, dass der Leiter des administrativen Kontrollorgans den Weisungen des Präsidenten des Unabhängigen Kontrollrats im Sinne von § 41 Abs. 2 i. V. m. § 48 unterliegt, und nicht beispielsweise solchen des Präsidenten des BND. Dies stünde einer wirksamen Wahrnehmung von Kontrollaufgaben entgegen.

Die sachliche Zuständigkeit des administrativen Kontrollorgans wird mit dem vorliegenden Gesetzentwurf nicht hinreichend klar geregelt. Im Entwurf heißt es in § 51 Abs. 1 sinngemäß mehrfach „soweit nicht das gerichtsähnliche Kontrollorgan zuständig ist“ und es wird mit einer Rückausnahme gearbeitet wird. Nach Ansicht des eco gibt die vorliegende Regelung Anlass zu der Sorge, dass die administrative Rechtskontrolle einem stetigen Rechtfertigungszwang unterworfen ist, ob überhaupt deren Zuständigkeit eröffnet ist. Eine derartige Ausgestaltung ist für die Wahrnehmung einer tatsächlichen und wirksamen Kontrolle abträglich und kontraproduktiv. Unklar bleibt beispielsweise der Umfang der möglichen Prüfungen durch die administrative Rechtskontrolle, welche im Entwurf durch die gerichtähnliche Kontrolle näher geregelt werden soll.

Die in § 56 verfügte Pflicht des BND zur Unterstützung der Arbeit des unabhängigen Kontrollrates ist jedoch gekennzeichnet von Ausnahmen und Rückbezügen (vgl. Abs. 2., „soweit die Kontrollbefugnis reicht“, Abs. 3 „alleinige Verfügungsberechtigung“, „soweit dies zur Kontrolle erforderlich ist“), welche eine effektive Kontrolle erneut unmöglich machen würde.

IX. Regelung der Technischen Kontrolle unzureichend

eco sieht mit dem vorliegenden Gesetzentwurf den konkreten Umfang der technischen Kontrolle der Aufklärungstätigkeit des BND als unzureichend geregelt an. Unklar ist bereits die zuständige Stelle. Es ist unklar, ob das gerichtsähnliche oder das administrative Kontrollorgan zuständig ist (vgl. auch § 51 Abs. 1 S. 2). Nicht hinreichend konkret ist die personelle Ausstattung (fachlich d. Mitarbeiter) und sowie deren sachliche Ausstattung und die Befugnisse der Technischen Kontrolle. Nach Ansicht des eco würde es aus Gründen der besseren Transparenz notwendig und zweckmäßig, wenn in dem Gesetzentwurf die sachliche Zuständigkeit durch mehrere, konkrete Erwähnungen im Tatbestand präzisiert wird.

Dies bezieht sich unter anderem auf folgende Aspekte, die bei der tatbestandlichen Ausgestaltung von § 57 berücksichtigt werden sollten:

- die administrative Rechtskontrolle ist zuständig für die technische Kontrolle, einschließlich der Wirksamkeit der Filter zum Ausscheiden unzulässiger Datenerhebung bzw. deren automatischer Löschung

- die administrative Rechtskontrolle ist technisch und personell so auszustatten, dass sie ihre Aufgaben jederzeit wirksam wahrnehmen kann.

- die administrative Rechtskontrolle verfügt über mindestens 25 Mitarbeiter, die hinsichtlich ihrer jeweiligen Aufgaben über die erforderliche persönliche sowie fachliche Eignung verfügen.

X. Mangelende Transparenz über zukünftige Befugnisse

Für äußerst bedenklich erachtet eco das Vorgehen des Gesetzgebers, im Rahmen des Gesetzesvorhabens „Anpassung des Verfassungsschutzrechts“ [3] dem BND (und den Ämtern für Verfassungsschutz und dem MAD) die Befugnisse für die Quellen-Telekommunikations-überwachung und der Online-Durchsuchung einräumen zu wollen, ohne im hier zur Konsultation gestellten Entwurf einen ausdrücklichen Hinweis auf diese weitere geplante Änderung des G10-Gesetzes zu geben. Dies mag aus formellen Gründen zwar nicht erforderlich sein, allerdings würde es eine Gesamtbetrachtung der in den verschiedenen Gesetzentwürfen vorgehsehen Ermächtigungen und Befugnisse ermöglichen. Der vom Bundesverfassungsgericht angemahnten Transparenz entspricht es in keiner Weise.

XI. Verletzung des Zitiergebots (§ 68)

Nach Ansicht des eco bestehen erhebliche Mängel an der mit dem Gesetzentwurf vorgeschlagenen Neuregelung des Zitiergebots in § 68 BNDG-E. Zukünftig soll lediglich in

[3] O. g. Gesetz wurde am 21.10.2020 vom Bundeskabinett beschlossen.

einziger Norm lediglich formuliert werden, dass das Gesetz die Grundrechte einschränkt. Weder werden die eingreifenden Befugnisse des BND genannt noch die betroffenen Grundrechte. Weder wird dies der Warnfunktion an die jeweiligen Normanwender gerecht noch trägt es zur Verbesserung der Kontrolle des Dienstes bei. Vor dem Hintergrund der heimlichen Eingriffe des BND und fehlendem gerichtlichen Rechtsschutz ist die Beachtung des Zitiergebots unerlässlich. Keine taugliche Alternative für die Nennungen in allen jeweiligen Eingriffsnormen bietet insofern Art. 12 des RefE, der pauschal darauf hinweist, dass der Abschnitt 4 des Artikels 4 und das G-10-Gesetz-E den Art. 10 GG einschränken. Zudem zitieren weder § 68 noch Art. 12 das auf Recht auf informationelle Selbstbestimmung noch das daraus abgeleitete Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG. Deren etwaige Subsidiarität schließt Eingriffe durch die geregelten Maßnahmen nicht aus, aber noch Art. 10 GG als spezielleres Grundrecht berühren.

XII. Perpetuierung der verfassungswidrigen Rechtslage

Mit Übergangsregelungen nach § 69 Absätze 2, 3 wird nach Einschätzung des eco die verfassungswidrige Rechtslage nach den §§ 18, 19 und § 23 BNDG perpetuiert, ohne dass dies erforderlich oder gerechtfertigt wäre.

Aus verfassungsrechtlichen Gründen ist die in § 69 Abs. 5 angeordnete Weitergeltung bestehender Kooperationsvereinbarungen mit ausländischen öffentlichen Stellen bis längstens zum 31. Dezember 2024 nicht akzeptabel. Das heißt praktisch, alle Kooperationsvereinbarungen, die vor dem 01.01.2022 und vor dem In-Kraft-Treten der Regelungen nach den §§ 31 bis 34 zu Kooperationen nach dem vorliegenden Entwurf geschlossen wurden, unterliegen nach dem Willen des Gesetzgebers nicht den Vorgaben des BVerfG (1 BvR 2835/17, Rn. 243 - 264). Diese Vereinbarungen sollen aber trotzdem bis Ende 2024 weitergelten dürfen. eco hält das für unvereinbar mit der vom Gericht ausnahmsweise zugelassenen Anwendung der verfassungswidrigen Normen bis 31.12.2021. Die unter den grundgesetzwidrigen Regelungen geschlossenen Kooperationsvereinbarungen sind selbst nicht mit dem Grundgesetz vereinbar, und müssten daher bis Ende 2021 neu vereinbart werden.

XIII. Berücksichtigung anderer verfassungsrechtlicher Vorgaben

Nach Auffassung des eco sind die Vorgaben des Bundesverfassungsgerichts zur manuellen Bestandsdatenauskunft vom 27.05.2020, 1 BvR 1873/13 zu beachten. In den § 6 Absatz 1, § 10 Absatz 3, § 28 Abs. 4, § 40 Absätze 1 und 2 reicht jedoch weiterhin als Zweck die Erforderlichkeit zur Aufgabenerfüllung aus. Das Bundesverfassungsgericht hat klargestellt, dass je weiter die Befugnisse zur Aufklärung sind, desto mehr sind hinsichtlich des Zwecks verfassungsrechtliche Einhegungen durch Zweckbegrenzungen erforderlich.

XIV. Unzureichende Regelung zum Gegenstand der Evaluierung (§ 61)

Nach Ansicht des eco ist die Regelung in Satz 1 hinsichtlich des Gegenstands der Evaluierung nicht hinreichend konkret. eco regt an, den § 61 Satz 1 am Ende zu ergänzen, mit den Wörtern „insbesondere hinsichtlich der Praktikabilität der Regelungen, des vermeidbaren Erfüllungsaufwands, der Ausstattung personelle und sachlichen Mitteln zur Wahrnehmung wirksamer Kontrolle.“. Die vorgeschlagene Ergänzung konkretisiert den Gegenstand der Evaluierung und die Auflistung werden auch vom Gesetzgeber als geeignete Kriterien erachtet, vgl. Begründung zu § 61, S. 77 des RefE.

XV. Zusammenfassung

eco erkennt dringenden Verbesserungsbedarf an dem vorliegenden Gesetzesentwurf.

- In mehreren Vorschriften wird der Personenbezug von Daten gesetzgeberisch aufgehoben, ohne dass er tatsächlich entfiele, oder als nicht relevant definiert (§ 2 i. V. m. §§ 10-18). Das führt zu einer Ausweitung anstatt einer Einschränkung des BND bei der Verarbeitung dieser Daten.
- Hinsichtlich der strategischen Fernmelde-Aufklärung soll in zentralen Vorschriften und Ermächtigungsnormen, die unter anderem das staatliche Eindringen bzw. Hacken ausländischer Telekommunikations- und Telemedienanbieter ermöglicht, diese Befugnis lediglich qualifizierten Beschränkungen hinsichtlich Inhaltsdaten unterliegen, nicht aber für Verkehrs- und Metadaten (§ 19) gelten. eco lehnt das eine staatliche Befugnis zum Hacking unter Ausnützung von Softwarelücken grundsätzlich ab. Es führt zur Gefährdung der IT-Sicherheit, der Integrität von IT-System und schwächt die Vertrauenswürdigkeit von Kommunikation.
- Das Bundesverfassungsgericht hat dem Gesetzgeber bzgl. technischen Filtern vorgegeben, dass diese dem Stand der Wissenschaft und Technik zu entsprechen. Der Gesetzgeber bleibt hier deutlich hinter den verfassungsrechtlichen Anforderungen zurück, wenn er trotzdem den Stand der Technik als ausreichend erachten will.
- Die Eignungsprüfung (§ 24) unterliegt keiner wirksamen Kontrolle und ist de facto zeitlich unbegrenzt möglich.
- Bei der Verarbeitung von personenbezogenen Verkehrsdaten setzt der Gesetzgeber die normative Aufhebung des Personenbezugs, ohne dessen tatsächlichen Wegfall, fort (§ 26). Als gesetzliche Ausnahme werden damit faktisch Millionen Kommunikations-vorgänge als nicht menschliche Kommunikation definiert (z. B. Verkehrs- und Metadaten von Telefonaten, E-Mails, Messenger-Nachrichten, Surfen, Online-Banking, Naviga-tionsapplikationen, Hotelbuchungen) soweit die Daten nicht beim Sender oder Empfänger direkt abgefangen werden).
- Der vorliegende Entwurf perpetuiert nach Ansicht des eco die verfassungswidrige Rechtslage, indem mehrere Vorschriften direkt oder mittelbar über den 31.12.2021

hinaus angewendet werden sollen, teilweise sogar bis Ende 2024. Dies widerspricht dem Urteil des Bundesverfassungsgerichts erheblich (§ 68).

- Zudem beachtet der Gesetzgeber andere Vorgaben des Gerichts nicht, indem er in mehreren Normen die Erforderlichkeit zur Aufgabenerfüllung als Zweck ausreichen lässt. Dies ist nach dem Grundgesetz keine ausreichende Zweckbegrenzung (§§ 6, 10, 28, 40).

Über eco:

Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Die Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie eine ethisch orientierte Digitalisierung bilden Schwerpunkte der Verbandsarbeit. eco setzt sich für ein freies, technikneutrales und leistungsstarkes Internet ein.