

## Hauptkritik zum Gesetzesentwurf zur Reform des BND-G (BT-Drs. 19/ 26103)

Berlin, 18.02.2021

**Das Bundesverfassungsgericht hat dem Gesetzgeber aufgegeben, die Ausland-Ausland-Aufklärung verfassungsgemäß zu gestalten. Der vorliegende Gesetzesentwurf entspricht nicht den Vorgaben des Gerichts und schafft dazu neue Rechtslagen, die nicht verfassungskonform sind.**

Im Folgenden möchte eco seine wesentlichen Kritikpunkte an dem Gesetzentwurf noch einmal in den zentralen Punkten darlegen. Ergänzend möchten wir auf unsere ausführliche [Stellungnahme](#) zum Referenten-Entwurf des Kanzleramts vom 03.12.2020 verweisen, welche eine ausführliche Darstellung der einzelnen Kritikpunkte bietet.

### I. Kritische Aufhebung des Personenbezugs von Daten

eco lehnt die Aufhebung des Personenbezugs von Daten ab. Das Wort „Informationen“ darf in den §§ 10 – 18 nicht gestrichen werden. Anderenfalls unterliegt der BND bei der Verarbeitung von Informationen alleine den Beschränkungen von § 2 BNDG.

Die Aufhebung des Personenbezugs würde konkret bedeuten, dass:

- Kaum Beschränkungen des BND bei der Erfassung einer immensen Vielzahl von Lebenssachverhalten bestehen, so dass mitnichten von einer Ausnahme gesprochen werden kann (vgl. § 26 Abs. 3 S. 2 u. S. 3),
- Ebensowenig bestehen Schranken beim Einsatz untauglicher Mittel zur Entfernung des Personenbezugs (vgl. § 26 Abs. 2 S. 3),
- Insgesamt bestehen kaum Schranken bei der Erfassung und Verarbeitung, falls der BND seine Auslegung und Interpretation durchsetzen kann, es handele sich bei „nicht menschlicher Kommunikation“ nicht um personenbezogene Daten.

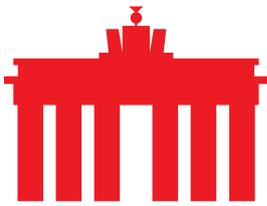
### II. Kritik an nahezu schrankenloser, strategischer Ausland-Fernmeldeaufklärung

eco lehnt den nahezu schrankenlosen Zugriff auf Daten, welche keine Inhaltsdaten sind, durch den BND gemäß § 19 Abs. 1 entschieden ab. Die Beschränkungen dieser Ermächtigung nach den Absätzen 2 bis 5 gelten nur für personenbezogene Inhaltsdaten. In der Konsequenz würde dies bedeuten, dass alle anderen Arten von Daten gem. § 2 BNDG mit technischen Mitteln verarbeitet bzw. erhoben werden dürften.

Nach Ansicht des eco stellt dies einen Verzicht auf konkretisierende Eingriffsschwelle dar und kommt einer Freistellung von einem Kernelement rechtsstaatlicher Anforderungen gleich. Das widerspricht den Vorgaben des Bundesverfassungsgerichts<sup>1</sup>.

---

<sup>1</sup> Vgl. 1 BvR 2835/17, Rn. 155.



### **III. Suchbegriffe nicht kontrollierbar**

Nach Auffassung des eco sind die Suchbegriffe weiterhin keiner wirksamen Kontrolle unterworfen. Die Definition von Suchbegriffen nach § 19 Abs. 5 muss eine wirksame Kontrolle eingesetzter Suchbegriffe ermöglichen. Beispielsweise könnte eine Prüfung derartiger Suchbegriffe im Rahmen der administrativen Kontrolle anhand statistischer Parameter zu dem jeweiligen Suchbegriff (z.B. konkrete Trefferzahl, Anzahl der Treffer je Anzahl Verkehre) bewertet werden, erfordert dabei aber neben der positiven auch eine negative Abschätzung der Wirkung des individuellen Suchbegriffes (z.B. unspezifische oder überbordende Anzahl von Treffern durch den jeweiligen Suchbegriff).

### **IV. Kritik am staatlichen Hacking**

eco bewertet die Befugnis zum staatlichen Hacking aus § 19 Abs. 6 grundsätzlich sehr kritisch. Gegenstand der Regelung ist der Zugriff des BND auf Bestands-, Verkehrs- und Inhaltsdaten ohne Wissen des jeweiligen Betreibers. Die Regelung ist auch auf Plattformbetreiber wie Google, Facebook, Amazon und Apple anwendbar. Grundsätzlich wären alle Dienstanbieter von Telekommunikation, Clouddiensten und sonstigen Telemediendiensten im Ausland potentielle Ziele eines staatlichen Eindringens. Betroffen sind hiervon regelmäßig auch die Mehrzahl der Bundesbürger, welche diese Dienste nutzen.

Dieser gesetzgeberische Ansatz bildet zur Umsetzung zudem einen massiven Anreiz für staatliche Akteure, Dienste und berechnete Stellen sich Informationen über 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 allgemein die Vertrauenswürdigkeit von Kommunikation und das Vertrauen in digitale Dienste.

### **V. Automatische Filtersysteme entsprechen nicht der Verfassung**

eco lehnt die geplante Regelung zu automatischen Filtersystemen ab. Die Regelung nach § 19 Abs. 7 S. 4 stellt einen Verfassungsbruch dar, indem ausschließlich auf den „Stand der Technik“ abgestellt und dieser als ausreichend erachtet wird. Das BVerfG hat bewusst die Vorgabe gemacht, dass die einzusetzenden Filtersysteme dem Stand der Wissenschaft und Technik zu entsprechen haben (vgl. Rn. 173 v. 1 BvR 2835/17). Diese Vorgaben werden in dem Gesetzentwurf nicht berücksichtigt. Gem. § 19 Abs. 7 S. 4 wird lediglich der „Stand der Technik“ als ausreichend erachtet. Das BVerfG hat bewusst die höchste Anforderung für den Einsatz von Filtersystemen vorgegeben, wie sie beispielsweise auch im Atomgesetz vorgesehen und geregelt ist. Ein Abstellen auf den „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.

### **VI. Selbstrechtfertigende Gefahrenlagen**

eco hält es für dringend geboten, dass in § 19 Abs. 7 Satz 6 eine tatbestandliche Einschränkung vorgenommen und damit klargestellt wird, dass die tatsächlichen Anhaltspunkte für Gefahren nicht aus den vom BND erhobenen Daten nach § 19 Abs. 1 i. V. m. Abs. 7 S. 1 selbst stammen dürfen. Anderenfalls würden alle in § 19 Abs. 7 vorgesehenen einschränkenden Tatbestandsmerkmale obsolet und keinerlei begrenzende Wirkung entfalten.



## **VII. Erfassungsgrenze untauglich**

eco erachtet die Erfassungsgrenze in § 19 Abs. 8 auf 30% aller weltweiten Telekommunikationsnetze für keine taugliche Begrenzung der Erfassung.

Zur Veranschaulichung: In §10 Abs. 4 des G10-Gesetzes wird eine Grenze von 20% der dort gegenständlichen Inlands-Auslands-Datenverkehre der jeweils beschränkten Anzahl Übertragungswege einer einzelnen Anordnung als im Ansatz prüfbare Beschränkung gewählt.

Demgegenüber stellen 30% des Datenverkehre aller weltweiten Telekommunikationsnetze keine tatsächliche Beschränkung und insbesondere keine prüfbare Beschränkung dar. Weltweit bestehen derzeit rund 70.000 am internationalen Verkehr teilnehmende Datennetze, 30% dieser Datennetze würden mithin als „Grenze“ eine Überwachung von 20.000 gleichzeitig überwachbaren Datennetze begründen.

In der gesamten Bundesrepublik Deutschland bestehen derzeit rund 1.250 am internationalen Datenverkehr teilnehmende Datennetze, die geplante gesetzliche Grenze würde insofern die Überwachung von 16 mal dem gesamten Verkehr der Bundesrepublik Deutschland ermöglichen.

Zudem sind die Verkehre in den Datennetzen nicht gleichverteilt und deutlich von grossen Anbietern geprägt. In der Bundesrepublik würde die vollständige Überwachung von nur 10 Anbietern rund 99% aller Verkehre erfassen, auch bei einer weltweiten Betrachtung werden in den Top10 Datennetzen rund 95% aller Verkehre geführt, die Top25 tragen rund 99% aller Daten.

## **VIII. Keine Kennzeichnung bei Übermittlungen**

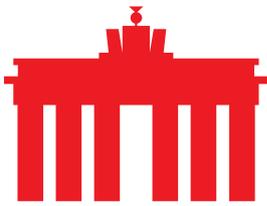
Nach Ansicht des eco sind die Regelungen zur Kennzeichnung von personenbezogenen Daten bei Übermittlungen des BND an andere Stellen unzureichend. Sie müssen so ausgestaltet werden, dass sie auch tatsächlich eine Wirkung entfalten können. Derzeit liefen die Regelungen weitgehend leer, da die anderen Stellen über die sich aus einem Personenbezug ergebenden Ausnahmen mangels Kennzeichnung keine Kenntnis haben können.

## **IX. Kontrollmöglichkeit nicht ausreichend**

eco ist der Auffassung, dass die Regelung des § 23 Abs. 6 S. 2 der Wahrnehmung einer wirksamen Kontrolle durch den unabhängigen Kontrollrat entgegensteht. Wenn Suchbegriffe nicht in der Anordnung genannt werden müssen, ist deren dauerhafte Speicherung für Kontrollzwecke anderweitig vorzusehen. Dies gilt auch für nur temporär verwendete Suchbegriffe. Ansonsten ist keine effektive Kontrolle gewährleistet, denn erst aus den Suchbegriffen ergibt sich die Zielgenauigkeit der Maßnahme.

## **X. Dauerhafte und unkontrollierte Eignungsprüfung**

Als Mindestanforderung muss die Eignungsprüfung des BND aus §24 wirksamen Schranken unterliegen, etwa der Genehmigung durch den Kontrollrat. Gegenwärtig werden weder Filtersysteme oder die Angabe von Suchbegriffe vorgegeben, noch Volumengrenzen. Im Vergleich zur bisherigen Rechtslage sind im Gesetzentwurf sogar Absenkungen der gesetzlichen Beschränkungen für den BND und damit folgende Ausweitungen vorgesehen:



- Nahezu beliebigen Datenspeicherung verschlüsselter Daten (§ 24 Abs. 1),
- zeitliche und administrative Öffnungsklausel, d. h. faktisch einen permanente Eignungsprüfung als dauerhaftes Instrument (§ 24 Abs. 2 S. 3 „mehrmalige Verlängerung“)
- keine Pflicht zur Benennung eines konkreten Telekommunikationsnetzes zur Erhebung der Daten (S. 70, BT-Drs.19/26103, Begründung zu § 24 Abs. 3).

Vor dem Hintergrund der Entscheidung des EuGH in der Rechtssache "Privacy International" (Az: C-623/17) sollten die Regelungen des § 24 zudem auf ihre generelle Vereinbarkeit mit Europarecht überprüft werden. In seiner Entscheidung hat der EuGH die EU-Rechtswidrigkeit nationaler Regelungen festgestellt, mit denen Betreiber elektronischer Kommunikationsnetze verpflichtet werden, in allgemeiner und unterschiedsloser Weise Verkehrs- und Standortdaten an Dienste und Sicherheitsbehörden zum Zwecke des Schutzes der nationalen Sicherheit zu übermitteln. Die in § 24 vorgesehene anlass- und unterschiedslose Ausleitung von Verkehren durch die Betreiber elektronischer Kommunikationsnetze fällt nach Ansicht des eco in den Anwendungsbereich der Entscheidung des EuGH und wäre insoweit nicht mit dem EU-Recht vereinbar. Die Regelung muss daher im Rahmen des parlamentarischen Verfahrens dringend angepasst werden, anderenfalls ist sie nicht mit dem EU-Recht vereinbar.

#### **XI. Personenbezug bleibt ohne Kennzeichnung unbekannt**

Wie bereits dargelegt sieht eco die gesetzlich fingierte Aufhebung des Personenbezugs von Daten kritisch. Die fehlende Kennzeichnung von personenbezogenen Daten in § 26 Abs. 2 ist deutlich einzuschränken. Die zukünftige Regelung würde dazu führen, dass alle Verkehrsdaten trotz des darin unzweifelhaft enthaltenen Personenbezugs zunächst ohne Kennzeichnung von Quelle oder Anordnungsgrundlage gespeichert werden dürften.

Eine entsprechende Kennzeichnung der Daten erst im weiteren Verlauf ist jedoch bereits offensichtlich unmöglich: Ohne sofortige Kennzeichnung ist die Quelle von Daten unbekannt. Eine manuelle Verarbeitung von Verkehrsdaten wie 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.

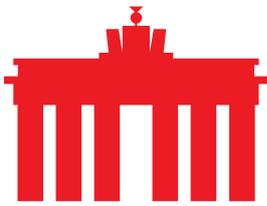
#### **XII. Unwirksame Anonymisierung von Verkehrsdaten aus In- und Auslandkommunikation**

eco erachtet die Regelung des § 26 Abs. 3 S. 2 Nr. 2 als dysfunktional. Eine Anonymisierung, wie darin vorgesehen, ist in technischer Hinsicht unmöglich solange auch nur ein Kommunikationsteilnehmer und ein weiteres eindeutiges Merkmal der Kommunikation bekannt sind. Eine derartige „Anonymisierung“ ist vielmehr durch eine einfache Datenkorrelation aufzuheben.

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

#### **XIII. Kritik an Aufhebung des Personenbezugs von Verkehrsdaten durch Gesetz**

eco sieht die gesetzliche Fiktion zur Aufhebung des Personenbezugs von Verkehrsdaten äußerst kritisch. Die Regelung des § 26 Absatz 3 Satz 2 Nr. 1 sowie Satz 4 sind zu streichen, damit nicht per gesetzlich fingierter Neudefinition der Personenbezug entfällt. Derzeit würde die Norm in der



Praxis millionenfach Lebenssachverhalte erfassen. Denn vielfach findet ein automatisierter Informationsaustausch statt, bspw. die Informationsbeschaffung im Internet, Online-Banking und Zahlungen, Hotelbuchungen, Navigationssysteme oder die GPS- und Bewegungsdaten von Mobilfunkgeräten, welche einen direkten Personenbezug aufweisen. Nach Einschätzung des eco würde die in dem Gesetzentwurf vorgesehene 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 wären dem BND hinsichtlich personenbezogener Verkehrsdaten keine praktisch wirksamen Grenzen oder Beschränkungen bezüglich einer Erhebung, Speicherung und Weiterverarbeitung von Verkehrsdaten von In- und Ausländern gesetzt.

#### **XIV. Hacking gefährdet IT-Sicherheit und schwächt Vertrauenswürdigkeit**

eco erachtet das Eindringen in IT-Systeme nach § 34 ebenfalls sehr kritisch. Wir nehmen Bezug auf die Ausführungen zu § 19 Abs. 6, da die Kritik gleichsam für das Eindringen in IT-Systeme einzelner Personen gilt. Die Grundproblematik bleibt, dass dadurch ein massiver Anreiz für staatliche Akteure, Dienste und berechnete Stellen besteht, sich Informationen über Softwarelücken in weitverbreiteten Anwendungen und System zu beschaffen und diese geheim zu halten. Dies schwächt allgemein die Vertrauenswürdigkeit von Kommunikation und das Vertrauen in digitale Dienste und darüber hinaus die IT-Sicherheit und die Integrität von IT-Infrastrukturen. Die Regelung steht in diametralem Gegensatz zu den Bemühungen des IT-SIG 2.0 oder der Neufassung der NIS-Richtlinie zur Erhöhung der IT-Sicherheit.

Der maximal zulässige Zeitraum nach § 34 Abs. 7 S. 2 von drei Jahren für eine Prüfung, ob die erhobenen Daten erforderlich sind, unangemessen lang.

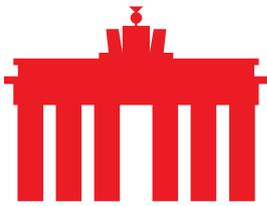
#### **XV. Regelung der Administrativen Rechtskontrolle unzureichend**

Nach Ansicht des eco sind die Regelungen zu konkretisieren. In § 50 muss 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. In § 51 Abs. 1 muss die sachliche Zuständigkeit des administrativen Kontrollorgans konkret und positiv geregelt werden. Diese sollte nicht mit der Ausnahme „soweit nicht das gerichtsähnliche Kontrollorgan zuständig ist“ und mit Rückausnahme geregelt werden. Es besteht Anlass zu der Sorge, dass die administrative Rechtskontrolle einem stetigen Rechtfertigungszwang unterworfen ist, ob überhaupt deren Zuständigkeit eröffnet ist.

Die in § 56 verfügte Pflicht des BND zur Unterstützung der Arbeit des unabhängigen Kontrollrates ist 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.

#### **XVI. Regelung der Technischen Kontrolle unzureichend**

eco sieht Nachbesserungsbedarf bei den Vorgaben zur Technischen Kontrolle. Ohne geeignete Vorgaben ist der konkrete Umfang der technischen Kontrolle der Aufklärungstätigkeit des BND unzureichend geregelt. Unklar ist derzeit bereits die zuständige Stelle, denn es bleibt unklar, ob



das gerichtsähnliche oder das administrative Kontrollorgan im Einzelfall zuständig ist (vgl. auch § 51 Abs. 1 S. 2). Nicht hinreichend konkret geregelt ist zudem die personelle Ausstattung (Fachkenntnis d. Mitarbeiter) und sowie deren sachliche Ausstattung und die Befugnisse der Technischen Kontrolle.

Bei der Ausgestaltung von § 57 sollte insofern geregelt werden:

- 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.

### **XVII. Verletzung des Zitiergebots**

Nach Ansicht des eco bestehen erhebliche Mängel an der mit dem Gesetzentwurf vorgeschlagenen Neuregelung des Zitiergebots in § 68 BNDG-E. Zukünftig soll lediglich in einer Norm formuliert werden, dass das Gesetz die Grundrechte einschränkt. Weder werden die eingreifenden Befugnisse des BND genannt noch die betroffenen Grundrechte. Dieses Vorgehen wird weder der Warnfunktion an die jeweiligen Normanwender gerecht noch trägt es zur Verbesserung der Kontrolle des Dienstes bei. Vor dem Hintergrund des bei heimlichen Eingriffen des BND fehlenden oder zumindest stark eingeschränkten gerichtlichen Rechtsschutzes ist die Beachtung des Zitiergebots unerlässlich.

### **XII. Perpetuierung der verfassungswidrigen Rechtslage**

Mit den Übergangsregelungen nach § 69 Abs. 2, Abs. 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 abzulehnen.

Dies vorgelegte Regelung hiesse praktisch, dass 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, nach dem Willen des Gesetzgebers nicht den Vorgaben des BVerfG (1 BvR 2835/17, Rn. 243 - 264) unterliegen.

#### 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.