REPORTER OHNE GRENZEN

Stellungnahme

zum Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts

Christian Mihr, Geschäftsführer Politik und Strategie, Reporter ohne Grenzen
Maximilian Jung, Referent Advocacy, Reporter ohne Grenzen

Niko Härting, Partner, HÄRTING Rechtsanwälte

Einreichung am 14.07.2026

Reporter ohne Grenzen (RSF) dokumentiert Verstöße gegen die Presse- und Informationsfreiheit weltweit und alarmiert die Öffentlichkeit, wenn Journalist*innen oder deren Mitarbeitende in Gefahr sind. Wir setzen uns für mehr Sicherheit und besseren Schutz von Medienschaffenden ein. Wir kämpfen online wie offline gegen Zensur, gegen den Einsatz sowie den Export von Überwachungstechnik und gegen restriktive Mediengesetze.

INHALT

Einleitung

Reporter ohne Grenzen (RSF) dankt für die Möglichkeit zur Stellungnahme zum Referentenentwurf vom 03.07.2026. Gleichwohl merken wir jedoch kritisch an, dass die knapp bemessene Frist von zehn Tagen für die sorgsame und tiefgründige Kommentierung des vorliegenden 707-seitigen Gesetzentwurfs nicht unseren Ansprüchen an eine angemessene, demokratische Verbändebeteiligung genügt.

Novellierungen des Nachrichtendienstrechts haben eine hohe Grundrechtsrelevanz. Insbesondere vor dem Hintergrund der groß angelegten Reform sowohl des Bundesamtes für Verfassungsschutz als auch des Bundesnachrichtendienstes sowie der umfassenden Umgestaltung ihrer Kontrolle durch die Zusammenführung beim Unabhängigen Kontrollrat ist eine gründliche Prüfung dringend geboten. Erschwerend kommt hinzu, dass vergangene Reformen des Bundesnachrichtengesetzes verfassungswidrige Regelungen hervorgebracht haben, die Teile der jetzigen Reform notwendig gemacht haben.

Reporter ohne Grenzen erkennt an, dass sich die sicherheitspolitische Lage in den vergangenen Jahren spürbar verändert hat. Hybride Bedrohungen, staatlich gesteuerte Desinformationskampagnen, Cyberangriffe auf kritische Infrastrukturen und eine zunehmend aggressive nachrichtendienstliche Tätigkeit fremder Mächte gegenüber Deutschland und seinen Verbündeten stellen die Nachrichtendienste vor neue Herausforderungen, denen der Gesetzgeber mit einer verlässlichen Rechtsgrundlage begegnen muss. Auch die Notwendigkeit der Reform als solche steht außer Frage: Das Bundesverfassungsgericht hat mit Beschluss vom 8. Oktober 2024 Teile der bisherigen strategischen Fernmeldeaufklärung für teilweise verfassungswidrig erklärt und dem Gesetzgeber eine Nachbesserungsfrist bis Ende 2026 gesetzt. Reporter ohne Grenzen begrüßt daher grundsätzlich, dass der Entwurf mehr Normenklarheit anstrebt, als es die bisherige, über mehrere Gesetze verstreute Rechtslage bot. Eine wirksame Reform darf jedoch nicht bei der institutionellen Neuordnung stehen bleiben, sondern muss diese Gelegenheit nutzen, um den Schutz besonders grundrechtssensibler Bereiche zu stärken statt abzusenken. Genau hier bestehen aus Sicht von Reporter ohne Grenzen erhebliche Defizite, die diese Stellungnahme im Einzelnen darlegt: Der Schutz journalistischer Vertraulichkeitsbeziehungen wird durch weit gefasste Ausnahmetatbestände in § 22 BNDG-E und § 32 BVerfSchG-E ausgehöhlt (1.), der Einsatz staatlicher Trojaner gegen Journalistinnen und Journalisten unterliegt keiner wirksamen Verhältnismäßigkeitsprüfung und keiner unabhängigen Vorabkontrolle (2.), die strategische Aufklärung wird ausgeweitet mit der neuen sechsmonatigen Speicherfrist für Inhaltsdaten und verliert mit dem Wegfall von Volumengrenze, Suchbegriffsverbot und Zweckkatalog wesentliche, bislang im G-10-Gesetz verankerte Schutzmechanismen (3.), und der neue Unabhängige Kontrollrat ist trotz erheblich erweiterter Zuständigkeit strukturell zu schwach ausgestattet, um diese Defizite auszugleichen – zumal die vorgesehene Einschränkung des Informationsfreiheitsgesetzes auch die externe, journalistische Kontrolle der Kontrolleure selbst erschwert (4.).

Die in dieser Stellungnahme vorgebrachte Kritik ist keineswegs erschöpfend. Reporter ohne Grenzen behält sich vor, zu einem späteren Zeitpunkt des Gesetzgebungsverfahrens ausführlicher Stellung zu beziehen.

1. Zum Schutz von Vertraulichkeitsbeziehungen

Reporter ohne Grenzen kritisiert insbesondere § 22 des Entwurfs zum BNDG (im Folgenden: BNDG-E), der den Schutz von Vertraulichkeitsbeziehungen für Journalistinnen und Journalisten sowie weitere besonders geschützte Berufsgruppen regeln soll.

In der Gesetzesbegründung (S.445f.) zur Norm wird ein zentrales Produkt der Organisation - die Rangliste der Pressefreiheit - als Hilfsmittel angeführt, um den Stand der Pressefreiheit eines Landes zu bewerten. Aus der Bewertung eines Landes mit sehr ernster Lage sei pauschal abzuleiten, dass Vertreter staatlicher oder staatlich gelenkter Presseeinrichtungen nicht als Journalistinnen und Journalisten gelten, sondern als „verlängerter Arm ihrer diktatorischen Regierung." Für sie gelte somit nicht der Schutz der Pressefreiheit, der Schutzbereich des § 22 BNDG-E würde nicht eröffnet.

Ziel der jährlichen Rangliste der Pressefreiheit ist es, den Grad der Pressefreiheit von Medienschaffenden und Medien in 180 Ländern oder Gebieten zu vergleichen. Sie folgt einer transparenten wissenschaftlichen Methodik und dient als zivilgesellschaftliches Analyse- und Advocacy-Instrument dazu, die weltweite Lage der Pressefreiheit zu dokumentieren, Missstände in repressiven Kontexten anzuprangern und diese nicht zuletzt durch internationalen Druck zu verbessern. Für diesen Zweck ist sie konzipiert, nicht als hoheitliches Einstufungsinstrument, das über die Reichweite grundrechtlichen Schutzes entscheidet.

Daran ändert auch der Umstand nichts, dass die Gesetzesbegründung kritische Journalistinnen und Journalisten aus den betreffenden Staaten vom Ausschluss ausnimmt. Denn der methodische Einwand bleibt bestehen: Die Rangliste bewertet die strukturellen Bedingungen der Pressefreiheit in einem Land. Sie trifft keine Aussage über einzelne Personen und ist dafür weder angelegt noch geeignet. Ob eine bestimmte Person journalistisch tätig und damit schutzwürdig ist, lässt sich aus einer Länderbewertung nicht ableiten. Der Entwurf verlangt der Rangliste damit eine Leistung ab, die sie nicht erbringen kann, und verlagert eine grundrechtserhebliche Entscheidung auf ein Instrument, das dafür nicht geschaffen wurde. Die Rangliste zur Begründung von Grundrechtseingriffen heranzuziehen, widerspricht ihrer Funktion: Ein Instrument, das staatliches Handeln kritisch begleiten soll, würde so zum Baustein eben dieses staatlichen Handelns. Reporter ohne Grenzen verwahrt sich gegen einen solchen Einsatz.

Ebenso sollen unterstützend für die Bewertung freier Journalismus versus staatlicher Propaganda journalistische Standards wie die Journalism Trust Initiative (JTI) herangezogen werden. Reporter ohne Grenzen begrüßt dies ausdrücklich unter der Maßgabe, dass es das Schutzniveau für Medienschaffende ausweitet. Die JTI ist ein öffentlich zugänglicher, maschinenlesbarer und zertifizierbarer Standard, der 2019 vom Europäischen Kommitee für Normung (CEN) als Workshop Agreement (CWA 17493) veröffentlicht wurde und dessen Zertifizierung durch akkreditierte Stellen nach ISO/IEC 17065 erfolgt - mit dem Ziel vertrauenswürdigen Journalismus auszuzeichnen. Er setzt nicht auf Ebene einer inhaltlichen Bewertung an. Vielmehr untersucht der Prüfkatalog Medienhäuser auf ihre ethischen Prinzipien, anerkannte journalistische Prozesse, wie beispielsweise das Zwei-Quellen-Prinzip, und Unabhängigkeitsgarantien. Die Heranziehung der JTI kann den Schutz nach § 22 sinnvoll erweitern, weil sie vertrauenswürdigen Journalismus anhand überprüfbarer, öffentlich zugänglicher Kriterien von getarnter Propaganda unterscheidet. Sie kann diese Abgrenzung aber nicht abschließend leisten: Als freiwilliger, auf Medienhäuser

bezogener Standard erfasst sie gerade kleine, neue oder unter Repression arbeitende Redaktionen und einzelne Journalistinnen und Journalisten oft nicht, obwohl diese besonders schutzbedürftig sind. Eine fehlende Zertifizierung stellt daher keinen hinreichenden Grund für die Verweigerung des Schutzes nach § 22 dar; insbesondere freie Journalistinnen und Journalisten oder solche, die aus Kriegs- und Krisengebieten berichten, haben sicher andere Sorgen und Nöte, als sich um eine Zertifizierung zu kümmern.

Bemerkenswert ist insoweit ein Widerspruch innerhalb der Gesetzesbegründung selbst: Sie stellt zunächst klar, dass es für die Zugehörigkeit zu den geschützten Berufsgruppen gerade „nicht auf die Berufsbezeichnung oder eine staatliche Zertifizierung" ankomme, sondern auf die tatsächlichen Gegebenheiten. Wenige Absätze später führt sie mit der JTI dann doch ein Zertifizierungsinstrument als Auslegungshilfe ein. Beides zusammen zeigt, dass der Entwurf die Frage, wer als geschützter Journalist gilt, nicht selbst beantwortet, sondern an externe Instrumente delegiert. Die JTI kann daher nur als unterstützendes Positivindiz dienen, dessen Vorliegen für die Schutzwürdigkeit spricht; ihr Fehlen darf den Schutz nicht schmälern. Die grundrechtserhebliche Entscheidung, wer als geschützte Journalistin oder Journalist gilt, muss der Gesetzgeber mit hinreichend bestimmten Kriterien im Gesetz selbst treffen.

Andere Rechtsordnungen kommen ohne solche Hilfskonstruktionen aus. Das französische Recht schützt Journalistinnen und Journalisten unmittelbar kraft ihrer Berufsausübung, ohne sie auf eine Zertifizierung oder ein Register zu verweisen.

Zu weit gefasste Eingriffsschwellen im BNDG-E

§ 22 BNDG-E ersetzt zum einen den bisherigen § 21 BNDG, der bislang für die Verarbeitung von Daten bei der Kommunikation ausländischer Personen im Ausland (sog. Ausland-Ausland-Kommunikation) galt. Zum anderen soll die Norm für die Kommunikation zwischen Personen im Ausland und Inland gelten (sog. Ausland-Inland-Kommunikation). Somit tritt § 22 BNDG-E für Journalist*innen an die Stelle des § 3b Abs. 2 und 4 des G10-Gesetzes (im Folgenden: G 10). Durch die Erfassung der Ausland-Ausland- sowie der Ausland-Inland-Kommunikation ist der Anwendungsbereich des § 22 BNDG-E somit außerordentlich weit gefasst.

§ 22 Abs. 1 BNDG-E untersagt zwar grundsätzlich die gezielte Erhebung personenbezogener Daten aus journalistischen Vertraulichkeitsbeziehungen. Der in Absatz 2 vorgesehene Ausnahmekatalog ist jedoch so weit gefasst, dass er das Regel-Ausnahme-Verhältnis des Absatzes 1 gegenüber der bisherigen Rechtslage praktisch umkehrt. Nach geltendem Recht waren Eingriffe in den Schutz journalistischer Vertraulichkeitsbeziehungen im Bereich der Ausland-Ausland-Kommunikation nur unter engen Voraussetzungen zulässig. Nach § 21 Abs. 2 Nr. 1 i.V.m. § 11a Abs. 1 BNDG musste die betroffene Person Täter oder Teilnehmer einer schweren Straftat oder einer Straftat im unmittelbaren Zusammenhang mit einem nachrichtendienstlich relevanten Gefahrenbereich – etwa der Gefährdung kritischer Infrastrukturen – sein. Alternativ musste nach § 21 Abs. 2 Nr. 2 BNDG die Maßnahme zur Abwehr einer Gefahr für ein besonders gewichtiges Rechtsgut, etwa Leib oder Leben, erforderlich sein.

Der Gesetzentwurf senkt diese Eingriffsschwelle erheblich ab. Künftig ist eine Beteiligung an einer Straftat nicht mehr erforderlich. Nach § 22 Abs. 2 Nr. 1 BNDG-E genügt vielmehr bereits, dass eine Person in einer beliebigen Weise mit einer „erheblichen Bedrohung“ im Sinne des § 3 Abs. 1 BNDG-E in Verbindung steht. Neben Personen, die selbst für eine

solche Bedrohung verantwortlich sind, erfasst die Vorschrift auch Mitglieder eines die Bedrohung unterstützenden Netzwerks.

Besonders weit gefasst ist jedoch § 22 Abs. 2 Nr. 1 lit. c BNDG-E. Danach reicht bereits ein „Zusammenhang […], der „Grund zu der Annahme gibt, dass durch die Maßnahme Erkenntnisse über diese Bedrohung gewonnen werden können, die nicht gleichermaßen durch eine Maßnahme gegen eine Person nach Buchstaben a und b zu gewinnen sind“. Hierbei nennt die Vorschrift explizit Personen, die Mitteilungen für entsprechende Personen entgegennehmen oder weitergeben, ohne dass dabei ein entsprechendes Bewusstsein vorausgesetzt wird. Gerade für Journalistinnen und Journalisten eröffnet diese Regelung ein erhebliches Überwachungspotenzial. Organisationen wie Reporter ohne Grenzen, die aufgrund ihrer Tätigkeit naturgemäß zahlreiche internationale Kontakte unterhalten und mit Personen aus sensiblen Kontexten oder Krisengebieten kommunizieren können, geraten dadurch strukturell in den Anwendungsbereich der Norm. Problematisch ist insbesondere, dass der Entwurf den Nachweis eines konkreten Kontakts zu einer tatsächlich bedrohungsrelevanten Person nicht fordert. Bereits die bloße Möglichkeit, aufgrund der Art der journalistischen Tätigkeit Erkenntnisse über eine erhebliche Bedrohung gewinnen zu können, kann somit für den erforderlichen „Zusammenhang […], der Grund zu der Annahme gibt“, ausreichen. Damit droht die Ausnahme zur Regel zu werden.

Besonders gravierend sind die Auswirkungen auf die Überwachung der Ausland-Inland-Kommunikation, also vor allem Journalisten und Journalistinnen, die von Deutschland aus mit Gesprächspartnern im Ausland kommunizieren. Bislang war nach § 3b Abs. 2 G 10 bei Überwachungsmaßnahmen gegen diese eine besondere Verhältnismäßigkeitsprüfung erforderlich. Abseits davon waren Maßnahmen nach § 3b Abs. 4 G 10 lediglich zulässig, wenn die betroffene Person selbst einer Straftat verdächtig war oder diese bewusst unterstützte. Der Gesetzentwurf gibt diese hohe Eingriffsschwelle auf.

Zum einen genügt künftig bereits gem. § 22 Abs. 2 Nr. 1 BNDG-E – wie schon bei der Ausland-Ausland-Kommunikation – ein bloßer Zusammenhang mit einer erheblichen Bedrohung oder die Annahme, dass über die betroffene Person relevante Erkenntnisse gewonnen werden könnten. Ob Journalistinnen und Journalisten tatsächlich im Bewusstsein handeln, eine verdächtige Person zu unterstützen, spielt somit keine Rolle mehr. Damit verschiebt sich die Eingriffsschwelle von einer bewussten Beteiligung an einer konkreten Rechtsgutsgefährdung hin zu einem äußerst weit gefassten Zusammenhangsbegriff.

Zum anderen genügt nach § 22 Abs. 2 Nr. 2 BNDG-E für Maßnahmen der Ausland-Inland-Kommunikation bereits, dass diese – wie bislang nur bei der Ausland-Ausland-Kommunikation nach § 21 Abs. 2 Nr. 2 BNDG – „zur Abwendung einer erheblichen Gefahr für ein besonders gewichtiges Rechtsgut“ notwendig sind. Was als „notwendig“ gilt, bestimmt der BND dabei im Wesentlichen selbst. Die Vorschrift verlagert die Grenzen zulässiger Überwachung damit in erheblichem Umfang in den Beurteilungsspielraum des Nachrichtendienstes und eröffnet ein erhebliches Missbrauchspotenzial. Besonders problematisch ist die Angleichung der Ausland-Inland-Kommunikation an das bislang deutlich niedrigere Schutzniveau der Ausland-Ausland-Kommunikation. Für in Deutschland tätige Journalistinnen und Journalisten mit internationalen Kontakten bedeutet dies einen Paradigmenwechsel: Vertrauliche journalistische Kommunikation wird nicht länger als besonders schutzwürdig behandelt, sondern gerät zum Regelfall potentieller nachrichtendienstlicher Überwachung.

Für den journalistischen Quellenschutz bedeutet dies eine strukturelle Schwächung: Statt eng begrenzter Ausnahmen eröffnet der Gesetzentwurf einen deutlich erweiterten Überwachungsrahmen, der journalistische Tätigkeit und den Schutz vertraulicher Quellen nachhaltig gefährdet. Umso schwerer wiegt, dass die Gesetzesbegründung zu § 22 Abs. 2 BNDG-E (S. 446) hierzu schweigt. Eine so weitreichende Ausweitung der Überwachung hätte einer ausdrücklichen Begründung und Auseinandersetzung bedurft.

Der Gesetzentwurf nutzt die Zusammenführung von BND-Gesetz und G-10-Gesetz in § 22 BNDG-E, um das Schutzniveau für journalistische Vertraulichkeitsbeziehungen bei der Ausland-Inland-Kommunikation an das deutlich niedrigere Niveau der bisherigen Ausland-Ausland-Kommunikation anzugleichen. In Deutschland tätige Journalistinnen und Journalisten unterliegen folglich denselben laxen Eingriffsvoraussetzungen wie zuvor nur ausländische Journalistinnen und Journalisten im Ausland. Richtigerweise hätte die Vereinheitlichung der beiden Regelungsregime jedoch in die entgegengesetzte Richtung erfolgen müssen: Statt das bislang für die Ausland-Inland-Kommunikation geltende, durch eine konkrete Straftatbeteiligung oder bewusste Unterstützung geprägte Schutzniveau des G10-Gesetzes abzusenken, hätte der Gesetzgeber dieses höhere Schutzniveau konsequent auf die gesamte Kommunikation zwischen Journalistinnen und Journalisten und ihren Quellen ausweiten müssen. Der Gesetzentwurf verpasst damit die Chance, den durch die Verfassungsgerichtsrechtsprechung ohnehin gebotenen Systemwechsel zu nutzen, um den Journalistinnenschutz in beiden Konstellationen auf ein einheitlich hohes Niveau zu heben; stattdessen wird die Vereinheitlichung zulasten der Pressefreiheit vorgenommen und der bislang bestehende, wenn auch nicht lückenlose, Schutz der Ausland-Inland-Kommunikation faktisch preisgegeben.

Ins Leere laufende Schutzvorkehrungen im BVerfSchG-E

Des Weiteren hegt Reporter ohne Grenzen Bedenken hinsichtlich der inhaltlich verwandten Vorschrift des § 32 BVerfSchG-E. Diese regelt den Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger – darunter Journalistinnen und Journalisten – im Bereich der Maßnahmen des Verfassungsschutzes. Nach § 32 Abs. 2 Satz 2 BVerfSchG-E sollen Maßnahmen gegen Journalistinnen und Journalisten zulässig sein, wenn sie der Aufklärung wenigstens erheblich beobachtungsbedürftiger Bedrohungen dienen und keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht. Beide Voraussetzungen vermögen den Eingriff jedoch kaum wirksam zu begrenzen.

So stellt bereits die erste Voraussetzung keine echte Einschränkung dar. Für „erheblich beobachtungsbedürftige Bedrohungen“ bedarf es gem. § 3 Abs. 7 Satz 1 BVerfSchG-E lediglich der Eignung der Bedrohung, die in § 2 Abs. 1 BVerfSchG-E genannten Schutzgüter erheblich zu gefährden. Gerade eine solche Gefährdung bildet jedoch ohnehin erst den typischen Anlass für das Tätigwerden des Verfassungsschutzes. Die Voraussetzung vermag den Anwendungsbereich der Vorschrift daher praktisch nicht einzugrenzen.

Nicht minder weit gefasst ist die zweite Voraussetzung. Anders als die bisherige Regelung des § 3b Abs. 2 G 10 verlangt § 32 Abs. 2 Satz 2 Nr. 2 BVerfSchG-E keine echte Verhältnismäßigkeitsprüfung mehr. Vielmehr soll die Maßnahme lediglich dann unzulässig sein, wenn der entstehende Nachteil erkennbar außer Verhältnis zum angestrebten Erfolg steht. Durch das zusätzliche Tatbestandsmerkmal der Erkennbarkeit wird die gerichtliche und behördliche Prüfung auf Fälle evidenter Unverhältnismäßigkeit reduziert. Die bislang erforderliche ausgewogene Abwägung zwischen dem öffentlichen Aufklärungsinteresse und

dem besonderen Gewicht des journalistischen Quellenschutzes wird damit erheblich abgeschwächt. Konträr hierzu beschränkt sich die Gesetzesbegründung zu § 32 Abs. 2 BVerfSchG-E (S. 313) allein darauf, zu konstatieren, dass § 32 Abs. 2 BVerfSchG-E lediglich die bisherige allgemeine Abwägungsformel konkretisiere. Ferner wird schlicht behauptet, § 32 Abs. 2 Satz 2 Nr. 2 BVerfSchG-E entspreche der bisherigen Regelung des § 3b Abs. 2 G 10. Dies lässt – bewusst oder unbewusst – außer Acht, dass der bisherige Schutzstandard nicht fortgeführt, sondern verengt wird. Indem die Zulässigkeit einer Maßnahme bereits dann bejaht wird, sofern ihre Unverhältnismäßigkeit nicht erkennbar ist, verschiebt sich der gesetzliche Regelungsansatz grundlegend. Die Schutzvorschrift entwickelt sich von einer echten Schranke nachrichtendienstlicher Maßnahmen zu einer Art Evidenzkontrolle, sodass die Zulässigkeit der Überwachung auch hier faktisch zum Regelfall wird.

Dass der Gesetzentwurf Quellenschutz durchaus ernst nehmen kann, wenn er will, zeigt sich im Übrigen an anderer Stelle: Für die eigenen menschlichen Quellen des Verfassungsschutzes sieht der Entwurf einen weitreichenden, praktisch lückenlosen Schutz vor, der ihre Identität und Zusammenarbeit selbst gegenüber den Mitteilungspflichten an die eigenen Kontrollorgane und an Betroffene ausnahmslos abschirmt, weil bereits der bloße subjektive Eindruck mangelnder Vertraulichkeit die Bereitschaft zur Zusammenarbeit gefährden könnte. Es ist nicht nachvollziehbar, weshalb der Gesetzgeber die Vertraulichkeit der eigenen Informantinnen und Informanten für derart schutzwürdig hält, während er den Quellen der Presse, die eine vergleichbare, verfassungsrechtlich verbürgte Funktion für die demokratische Öffentlichkeit erfüllen, lediglich eine im Ergebnis wirkungslose Abwägungsklausel zubilligt.

Ein Schutzmechanismus, der unter diesen Voraussetzungen im Ergebnis leerläuft, wird der verfassungsrechtlichen Bedeutung des journalistischen Quellenschutzes für die Funktionsfähigkeit einer freien Presse nicht gerecht. Reporter ohne Grenzen fordert daher, Berufsgeheimnisträger im Sinne des § 53 Abs. 1 Satz 1 Nummer 5 StPO – mithin Journalistinnen und Journalisten – aus dem Anwendungsbereich des § 32 Abs. 2 BVerfSchG-E herauszunehmen und ihnen stattdessen denselben Schutzstandard der restlichen Berufsgeheimnisträgerinnen und -trägern aus § 32 Abs. 1 BVerfSchG-E zuzubilligen. Nur ein kategorischer, nicht durch eine Einzelfallabwägung relativierbarer Erhebungsschutz wird der Tatsache gerecht, dass bereits die bloße Möglichkeit einer Überwachung ausreicht, um Informantinnen und Informanten von einer Zusammenarbeit mit der Presse abzuschrecken – ein Effekt, der sich durch die im Entwurf vorgesehene, faktisch konturenlose Abwägungsklausel nicht verhindern lässt.

Dass eine solche Gleichbehandlung möglich ist, zeigen andere Rechtsordnungen. Das französische Recht etwa unterwirft Maßnahmen gegen geschützte Berufsgruppen, darunter Journalistinnen und Journalisten, nach Art. L. 821-7 Code de la sécurité intérieure einem verschärften Verfahren: Die Kontrollkommission entscheidet in ihrer höchsten Besetzung, das Eilverfahren ist ausgeschlossen, und über die Durchführung der Maßnahme wird die Kommission unterrichtet.

Fortwirkender Schutz in der automatisierten Auswertung

Der Schutz journalistischer Vertraulichkeitsbeziehungen ist in § 22 BNDG-E und § 32 BVerfSchG-E auf die Datenerhebung zugeschnitten. Der Entwurf lässt in § 37 BVerfSchG-E jedoch erstmals ausdrücklich eine „qualifizierte Auswertung“ zu, die gespeicherte Daten durch automatisierte Verknüpfung zu neuen Erkenntnissen über die Persönlichkeit und die Beziehungen einer Person verdichtet, bis hin zu profilbildenden und „anpassungsfähig auf

einen autonomen Betrieb angelegten“ Verfahren; die §§ 52 ff. BNDG-E enthalten für den Bundesnachrichtendienst entsprechende Befugnisse. Für den journalistischen Quellenschutz liegt hierin ein eigenständiges Risiko: Das grundrechtlich maßgebliche Eingriffsgewicht entsteht nicht bei der Erhebung einzelner Daten, sondern erst bei ihrer Verknüpfung. Journalistische Arbeit ist naturgemäß durch eine Vielzahl von Kontakten in unterschiedlichste Milieus geprägt; in einer beziehungsanalytischen Auswertung können daraus Muster entstehen, die zu unzutreffenden Zuordnungen führen und die Identität von Quellen offenlegen, ohne dass ein einziger Kommunikationsinhalt gelesen wird. Der auf die Erhebung bezogene Schutz der §§ 22 BNDG-E und 32 BVerfSchG-E greift hier nicht, weil er in der automatisierten Weiterverarbeitung und Profilbildung nicht ausdrücklich fortwirkt. Hinzu kommt, dass sich ein System, das sein Verhalten im laufenden Betrieb verändert, durch eine einmalige Vorabkontrolle nicht abschließend prüfen lässt.

Dieses Regelungsdefizit betrifft im Kern das Recht der Öffentlichkeit auf verlässliche Information als Ausdruck der Pressefreiheit. Pressefreiheit schützt die Information entlang der gesamten Kette von der Entscheidung einer Quelle, diese weiterzugeben bis hin zur Rezeption durch die Öffentlichkeit. Diesem Verständnis zufolge dient der verfassungsrechtliche Schutz journalistischer Quellen in erster Linie nicht dem Individualinteresse Medienschaffender, sondern ist infrastrukturelle Voraussetzung für die demokratische Öffentlichkeit, die auf wahrheitsgemäße, verlässliche, und unabhängig recherchierte Berichterstattung angewiesen ist. Insbesondere investigative Recherchen zu Themen wie Rüstungsexporten, organisierter Kriminalität oder in Kriegs- und Konfliktsituationen liegen inhaltlich in unmittelbarer Nähe zu klassischen Aufklärungsinteressen der Nachrichtendienste und sind strukturell auf Informantinnen und Informanten angewiesen. Wie bereits weiter oben ausgeführt, und von der Gesetzgeberin selbst anerkannt, sind Quellen auf Zusicherung vollständiger Vertraulichkeit angewiesen, um ihr Wissen zu teilen. Lässt sich diese Vertraulichkeit im Wege automatisierter Datenanalyse untergraben, ohne dass die Erhebungsschutzvorschriften greifen, werden nicht nur einzelne Quellen gefährdet, sondern die Informationsgrundlage der gesamten Öffentlichkeit systematisch geschwächt. Wenn Informantinnen und Informanten dauerhaft befürchten müssen, algorithmisch-automatisiert enttarnt zu werden, versiegt der Informationsfluss, auf dem eine informierte demokratische Debatte ruht. Reporter ohne Grenzen fordert daher, den Schutz von Vertraulichkeitsbeziehungen auch auf die automatisierte Auswertung zu erstrecken und lernende Analyseverfahren einer begleitenden Kontrolle zu unterwerfen.

Präventive Enttarnung im Namen der Spionageabwehr

Weitergedacht gewinnt dieses Regelungsdefizit Bedeutung im Kontext der Spionageabwehr. Die neuen Auswertungsbefugnisse müssen in der nachrichtendienstlichen Arbeit gerade nicht nur auf die nachträgliche Aufklärung zur Enttarnung von Kontakten Anwendung finden, sondern können bereits - im Sinne des Predictive Policing - vorausschauend auf die Erkennung von Mustern und Verbindungen abzielen, um Erkenntnisse über eine bislang nicht nachrichtendienstlich als relevant eingestufte Person zu gewinnen (insb. § 53 Abs. 4 Nr. 2 i.V.m. Nr. 4 BNDG-E). Nach § 53 Abs. 4 Nr. 2 BNDG-E erfasst diese Kategorie ausdrücklich Auswertungsprodukte, die zur “Gewinnung von tatsächlichen Anhaltspunkten erstellt werden, dass eine Person, bei der individuell kein Anlass zur Prüfung bestand, in einem Zusammenhang mit einer zumindest erheblichen Bedrohung steht” und wird ergänzt durch personenbezogene Vorhersagen und Empfehlungen nach Nr. 4, die etwa automatisierte Auskunftsersuchen aufgrund eines Risikoprofils auslösen können.

Die Gesetzesbegründung (S. 536) betont selbst die grundrechtliche Sensitivität des Vorgangs, weil dieses Vorgehen “eine vormals unerkannte Person” gerade in den Fokus nachrichtendienstlichen Interesses rückt. Trotz dieser Einordnung begnügt sich die Gesetzgeberin aber mit der denkbar niedrigsten Eingriffsschwelle. Es reicht bereits ein Zusammenhang mit einer “zumindest erheblichen Bedrohung” - jener Schwelle also, die ohnehin erst den Anlass für nachrichtendienstliches Handeln bietet.

Schwerwiegender noch wiegt der strukturelle Widerspruch in der Logik der Norm. Zweck des Verfahrens nach §53 Abs. 4 Nr. 2 BNDG-E ist es ausdrücklich gerade “tatsächliche Anhaltspunkte” für einen Bedrohungszusammenhang bei einer Person zu gewinnen, die individuell keinen Anlass für eine Prüfung geboten hat. Zugleich macht §53 Abs. 4 Satz 1 BNDG-E die Zulässigkeit des Abrufs jenes Auswertungsproduktes von genau denselben tatsächlichen Anhaltspunkten für eine erhebliche Bedrohung abhängig. Um festzustellen, ob tatsächliche Anhaltspunkte für eine Bedrohung vorliegen, muss die Person also zunächst durch das System analysiert werden. Die Ergebnisse dieser Analyse liefert aber erst die Rechtfertigung für ihren eigenen Einsatz - ein Zirkelschluss.

Für die Spionageabwehr mag solch ein Instrument noch plausibel erscheinen, um anhand von risk scores den Abfluss von Informationen an gegnerische Nachrichtendienste frühzeitig zu unterbinden. Dieselbe Analytik lässt sich jedoch ohne Weiteres auf eine Person anwenden, deren Kommunikationsverhalten, Zugriffsmuster oder soziale Netzwerkstruktur Anlass bietet, sie als potenzielle Whistleblowerin einzustufen. Werden Ministerialbeamte, nicht nur der Nachrichtendienste, von einem automatisierten System bereits als auffällig markiert, bevor es überhaupt zur Kontaktaufnahme mit einer Journalistin oder einem Journalisten kommt, wird die Vertraulichkeitsbeziehung verhindert, ohne dass sie je entstanden ist. Die Schutzvorschriften der §§ 22 BNDG-E oder 32 BVerfSchG-E laufen doppelt ins Leere, denn sie beziehen sich auf eine bestehende journalistische Vertraulichkeitsbeziehung aus Sicht der Journalistin oder des Journalisten. Reporter ohne Grenzen möchte in diesem Zusammenhang das Recht, Quelle zu sein, ausdrücklich unterstreichen. Gerade weil sich politische Mehrheiten und die Ausrichtung staatlicher Stellen ändern können, sollte eine Sicherheitsarchitektur geschaffen werden, die verhindert, dass die abstrakte Überlegung eines künftigen Kontaktes zur Presse bereits einen Anlass zur nachrichtendienstlichen Vorfeldaufklärung bietet. Die Gesetzgeberin sollte sicherstellen, dass automatisierte Auswertungsverfahren zur Spionageabwehr nicht faktisch zu einem Instrument der vorbeugenden Quellenverhinderung werden.

2. Zu Trojanern

Nicht weniger besorgniserregend ist aus Sicht von Reporter ohne Grenzen die Regelung zum Eingriff in informationstechnische Systeme. RSF hat eine Beschwerde vor dem Europäischen Gerichtshof für Menschenrechte in Straßburg gegen die Regelungen zum Einsatz von Trojanern, den Mitteilungspflichten und dem Rechtswegausschluss aus § 11ff. G10 Gesetz eingelegt. Der entsprechende Fragenkatalog des Gerichts, in welchem grundsätzliche Fragen zu den Voraussetzungen des Eingriffs in informationstechnische Systeme und der IT-Sicherheit aller Bürgerinnen und Bürger aufgeworfen werden, die weit über den konkreten Klagegegenstand hinausweisen, wurde der Bundesregierung zugestellt. Die Gesetzgeberin verpasst es leider im Zuge der jetzigen Reform, diese Fragen proaktiv zu adressieren. Die neuen Vorschriften des § 35, §37f. BNDG-E mit § 100 f. und § 103 f. BNDG-E schreiben den von RSF bemängelten Zustand weiter fort. Mitteilungen an

betroffene Personen werden der Ausnahmefall bleiben; ohne eine solche bleibt den Betroffenen das Recht auf eine effektive Beschwerde und damit eine gerichtliche Nachkontrolle angeordneter Überwachungsmaßnahmen gegen sie praktisch verwehrt.

Nach wie vor fehlendes Schwachstellenmanagement

Kritikwürdig ist die in § 10 Abs. 2 Nr. 2 BNDG-E verankerte Pflicht des Bundesamts für Sicherheit in der Informationstechnik (BSI), dem BND proaktiv und ohne vorheriges Ersuchen Informationen zu übermitteln – wozu die Gesetzesbegründung (S. 411 f.) ausdrücklich auch Erkenntnisse über 0-Day-Schwachstellen zählt. Die Begründung macht dabei deutlich, worum es eigentlich geht: Der Zeitraum zwischen der Entdeckung einer Schwachstelle durch das BSI und deren Meldung an die Hersteller, der Bereitstellung eines Patches und dessen flächendeckender Installation soll dem BND als Zeitfenster dienen, um die Schwachstelle nachrichtendienstlich „in Wert zu bringen" – also offensiv auszunutzen, etwa im Rahmen der in §§ 36 ff. BNDG-E geregelten Online-Durchsuchung. Damit gerät die Vorschrift in einen fundamentalen Widerspruch zum eigentlichen gesetzlichen Auftrag des BSI, das nach dem BSI-Gesetz gerade für die Erhöhung der IT-Sicherheit in Deutschland und die zügige Behebung bekannter Schwachstellen zuständig ist. Anstatt dem Prinzip des „Responsible Disclosure" zu folgen und Schwachstellen schnellstmöglich an Hersteller zu melden, institutionalisiert der Entwurf faktisch eine Schwachstellenhortung zugunsten nachrichtendienstlicher Interessen – mit der Folge, dass ungepatchte Sicherheitslücken länger bestehen bleiben und damit auch für kriminelle Akteure oder gegnerische ausländische Nachrichtendienste angreifbar sind, die dieselbe Schwachstelle unabhängig entdecken könnten. Verschärft wird dies dadurch, dass das BSI – anders als etwa die Verfassungsschutzbehörden nach § 10 Abs. 4 Nr. 1 BNDG-E – von der Übermittlungspflicht nicht einmal dann befreit werden kann, wenn überwiegende Sicherheitsinteressen entgegenstehen: Der Gesetzentwurf sieht für das BSI keinerlei Ausnahme- oder Widerspruchsrecht vor, obwohl gerade hier eine Abwägung zwischen dem gesamtgesellschaftlichen Interesse an sicherer IT-Infrastruktur und dem nachrichtendienstlichen Interesse an der Offenhaltung von Angriffsvektoren evident geboten wäre. Dass die Gesetzesbegründung diesen Zielkonflikt zwar anspricht, ihn aber einseitig zugunsten der nachrichtendienstlichen Nutzung auflöst, ohne dabei ein höchstrichterlich gefordertes Schwachstellenmanagement zu implementieren (BVerfG, Urteil vom 08.06.2021 - 1 BvR 2771/18), offenbart ein strukturelles Defizit, das die Cybersicherheit der Allgemeinheit den operativen Interessen des BND unterordnet.

Diese Schwächung trifft journalistische Quellen in besonderem Maße. Wer sich entscheidet, Missstände offenzulegen, ist auf die Vertraulichkeit seiner Geräte angewiesen. Eine Sicherheitslücke, die der Staat bewusst offen hält, steht auch denen offen, vor denen sich Quellen schützen müssen.

Einsatz von Trojanern gegen (deutsche) Journalistinnen und Journalisten

Die Vorschrift des § 37 BNDG-E bildet zusammen mit § 38 BNDG-E die Nachfolgeregelung zu § 34 BNDG für Maßnahmen gegenüber der Ausland-Ausland-Kommunikation sowie zu § 11 Abs. 1a G 10 für Maßnahmen im Bereich der Ausland-Inland-Kommunikation. Zwar vermittelt der Gesetzentwurf auf den ersten Blick den Eindruck eines differenzierten und abgestuften Schutzkonzepts für Eingriffe in informationstechnische Systeme. Bei näherer

Betrachtung erweisen sich die vorgesehenen Schutzmechanismen jedoch als deutlich weniger wirksam, als es die Systematik der Vorschrift zunächst vermuten lässt.

Besonders deutlich wird dies am Beispiel eines deutschen Journalisten, dessen dienstlich genutztes Arbeitshandy mittels eines staatlichen Trojaners ausgespäht wird. Bei einem solchen Arbeitshandy handelt es sich um ein informationstechnisches System im Sinne der Vorschrift. Da das Gerät nicht dem privaten Bereich zugeordnet wird, ist allein § 37 Abs. 1 BNDG-E einschlägig. Die erhöhten Voraussetzungen der Absätze 2 und 3 greifen dagegen nicht ein, da diese ausschließlich für private informationstechnische Systeme vorgesehen sind. Dies hat zur Folge, dass für den Einsatz eines Trojaners gegen einen deutschen Journalisten bereits genügt, dass tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme erforderlich ist, um Informationen über zumindest erhebliche Bedrohungen im Sinne des § 3 Abs. 1 BNDG-E zu gewinnen.

Zwar definiert § 3 Abs. 1 BNDG-E eine erhebliche Bedrohung als eine Gefährdung, die geeignet ist, ein besonders gewichtiges Rechtsgut in besonderem Maße zu beeinträchtigen. Die eigentliche Eingriffsschwelle liegt jedoch nicht in diesem Bedrohungsbegriff, sondern in dem Merkmal der Erforderlichkeit. Gerade weil ein Trojaner aufgrund seines umfassenden Zugriffs auf gespeicherte und laufende Kommunikationsdaten regelmäßig das effektivste Mittel zur Informationsgewinnung darstellen wird, eröffnet die Vorschrift dem Bundesnachrichtendienst einen erheblichen Beurteilungsspielraum. Je weitreichender die technische Zugriffsmöglichkeit ist, desto leichter lässt sich argumentieren, dass gerade diese Maßnahme zur Erlangung relevanter Erkenntnisse erforderlich sei. Eine eigenständige Verhältnismäßigkeitsprüfung sieht § 37 Abs. 1 BNDG-E hingegen nicht vor. Dies überrascht umso mehr, als dem Gesetzgeber entsprechende Schutzmechanismen durchaus bekannt sind. So enthält etwa § 32 Abs. 2 Satz 2 Nr. 2 BVerfSchG-E zumindest noch Ansätze einer – wenn auch gegenüber der bisherigen Rechtslage bereits deutlich abgeschwächten – Verhältnismäßigkeitsprüfung (s.o.).

Diese niedrige Eingriffsschwelle steht in einem deutlichen Spannungsverhältnis zur außergewöhnlichen Eingriffsintensität der Maßnahme. Auf einem Arbeitshandy befinden sich regelmäßig zahlreiche personenbezogene Daten des betroffenen Journalisten. Hierzu zählen etwa Standortdaten, Fotos, Kalender- und Kontaktdaten sowie sonstige Informationen über seine beruflichen und privaten Lebensumstände. Von noch größerer Bedeutung ist jedoch die Möglichkeit, auf die Kommunikation mit journalistischen Quellen zuzugreifen. Gerade diese Kommunikation enthält häufig besonders sensible Informationen über Informantinnen und Informanten, deren Identität und deren vertrauliche Mitteilungen. Durch die Infiltration eines solchen Geräts werden daher sowohl das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG hinsichtlich laufender Kommunikation als auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hinsichtlich gespeicherter Daten in erheblichem Maße berührt. Problematisch erscheint in diesem Zusammenhang auch die gesetzgeberische Begründung der Differenzierung zwischen privaten und nicht privaten informationstechnischen Systemen. Die Gesetzesbegründung (S. 502) verweist insoweit auf die Entscheidung des Bundesverfassungsgerichts zum IT-Grundrecht (BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 und 1 BvR 595/07, BVerfGE 120, 274 ff., Rn. 206) und leitet daraus ab, dass allein privat genutzte informationstechnische Systeme in den Schutzbereich dieses Grundrechts fallen. Eine solche Lesart überzeugt jedoch nicht. Das

Bundesverfassungsgericht spricht allein davon, dass die betroffene Person das IT-System „überwiegend als eigenes nutzt“. Damit stellt es gerade nicht schematisch auf die Unterscheidung zwischen privaten und dienstlichen Geräten ab. Vielmehr knüpft es den Schutz an die berechtigte Erwartung der betroffenen Person, dass die Vertraulichkeit und Integrität des informationstechnischen Systems gewahrt bleibt. Eine solche Schutz- und Vertraulichkeitserwartung kann jedoch selbstverständlich auch bei einem dienstlich genutzten Arbeitshandy bestehen. Dies gilt insbesondere für Journalistinnen und Journalisten, deren berufliche Tätigkeit gerade auf vertraulicher Kommunikation mit Quellen beruht.

Nun könnte man auf den ersten Blick meinen, dass § 22 BNDG-E als zusätzliche Schutzvorschrift zu Hilfe kommt. Bei näherer Betrachtung erweist sich jedoch auch diese Hürde als begrenzt wirksam. Nach § 22 Abs. 1 BNDG-E ist die Erhebung personenbezogener Daten unzulässig, wenn sie zum Zweck der „gezielten“ Erlangung von Informationen aus einer journalistischen Vertraulichkeitsbeziehung erfolgt. Die Vorschrift schützt damit nur Maßnahmen, die gerade auf die Vertraulichkeitsbeziehung als solche gerichtet sind. Dem Bundesnachrichtendienst bleibt es demgegenüber möglich, die Maßnahme formal auf die Gewinnung sonstiger personenbezogener Daten auszurichten. Gelangen im Rahmen einer solchen Maßnahme zugleich Informationen aus der Kommunikation zwischen Journalist und Quelle ans Licht, greift das Verbot des § 22 Abs. 1 BNDG-E nicht ohne Weiteres ein. Der Schutz journalistischer Vertraulichkeitsbeziehungen droht dadurch in der praktischen Anwendung erheblich an Wirksamkeit zu verlieren.

Hinzu kommt, dass Maßnahmen nach § 37 Abs. 1 BNDG-E nicht einmal einer vorgelagerten Kontrolle durch den Unabhängigen Kontrollrat unterliegen. Nach § 97 Abs. 1 Nr. 14 BNDG-E besteht eine solche Vorabkontrolle lediglich für Maßnahmen nach § 37 Abs. 2 und 3 BNDG-E. Gerade die hier einschlägige Standardmaßnahme des § 37 Abs. 1 BNDG-E bleibt davon ausgenommen. Selbst die wenigen verbliebenen Kontrollmechanismen greifen somit nicht zugunsten des betroffenen Journalisten ein. Gleiches gilt für die Mitteilung an betroffene Personen nach § 100 Abs. 1 Nr. 2 BNDG-E. Wie bereits bei der Vorabkontrolle durch den Unabhängigen Kontrollrat, ist für die Standardmaßnahme nach § 37 Abs. 1 BNDG-E keine Mitteilungspflicht vorgesehen. Ohne eine solche bleibt dem betroffenen Journalisten auch nicht die Möglichkeit, die Maßnahme nachträglich vor Gericht überprüfen zu lassen.

Insgesamt bleibt zu bezweifeln, ob sich die Mitteilungspraxis des BND verbessert. Der BND kann mittels § 100 Abs. 4 Nr. 4 bereits von vornherein (ohne den Umweg über eine Zurückstellung) endgültig von einer Mitteilung absehen, wenn schon zu Beginn "mit an Sicherheit grenzender Wahrscheinlichkeit" feststeht, dass eine dauerhafte Nichtmitteilung geboten sein wird. Diese Feststellung ist zwar an die Zustimmung des Unabhängigen Kontrollrats gebunden, schafft aber einen zusätzlichen, in dieser Form bislang nicht existierenden Ausnahmetatbestand.

Der Europäische Gerichtshof für Menschenrechte verlangt demgegenüber in ständiger Rechtsprechung (grundlegend EGMR, Sanoma Uitgevers B.V. gegen die Niederlande [Große Kammer], Nr. 38224/03, Urteil vom 14. September 2010; fortgeführt in Telegraaf Media Nederland Landelijke Media B.V. u.a. gegen die Niederlande, Nr. 39315/06, Urteil vom 22. November 2012), dass vor dem gezielten Zugriff auf Material, das journalistische Quellen enttarnen könnte, eine unabhängige Stelle prüft, ob das öffentliche Interesse den

Quellenschutz ausnahmsweise überwiegt. Die Niederlande haben daraus Konsequenzen gezogen: Nach Art. 30 Abs. 2 der Wet op de inlichtingen- en veiligheidsdiensten 2017 bedarf die gezielte Überwachung journalistischer Kommunikation einer gesonderten, berufsspezifischen vorherigen Genehmigung durch die Rechtbank Den Haag.

Auch der Unionsgesetzgeber hat diesen Maßstab inzwischen festgeschrieben. Nach Art. 4 Abs. 3 Buchstabe c der Verordnung (EU) 2024/1083 (Europäisches Medienfreiheitsgesetz), die seit dem 8. August 2025 allgemein gilt, ist der Einsatz intrusiver Überwachungssoftware gegen Journalistinnen und Journalisten und ihre Kontaktpersonen grundsätzlich untersagt. Abweichungen sind nach Absatz 5 nur zulässig, wenn der Einsatz gesetzlich vorgesehen, verhältnismäßig und zur Aufklärung schwerer Straftaten erforderlich ist; er unterbleibt, wenn mildere Mittel ausreichen. Absatz 6 verlangt zudem, dass der Einsatz regelmäßig durch eine Justizbehörde oder ein unabhängiges und unparteiisches Entscheidungsgremium überprüft wird, und Absatz 8 gewährleistet den Betroffenen wirksamen gerichtlichen Rechtsschutz. § 37 Abs. 1 BNDG-E bleibt hinter jedem dieser Elemente zurück: Er sieht weder eine eigenständige Verhältnismäßigkeitsprüfung noch eine unabhängige Vorabkontrolle noch eine Mitteilungspflicht vor, die den gerichtlichen Rechtsschutz überhaupt erst ermöglichen würde.

Fazit

Insgesamt drängt sich daher der Eindruck auf, dass der Gesetzentwurf die verfassungsrechtliche Tragweite des Einsatzes staatlicher Trojaner gegenüber Journalistinnen und Journalisten erheblich unterschätzt. Die Kombination aus niedriger Eingriffsschwelle, fehlender Verhältnismäßigkeitsprüfung, eingeschränktem Schutz journalistischer Vertraulichkeitsbeziehungen und dem Fehlen einer unabhängigen Vorabkontrolle sowie der Mitteilungspflicht als Anstoß für eine ex-post Kontrolle eröffnet einen weitreichenden Überwachungsrahmen. Vor diesem Hintergrund bestehen erhebliche Zweifel an der Vereinbarkeit der Regelung mit dem Fernmeldegeheimnis aus Art. 10 Abs. 1 GG sowie dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

3. Zur „strategischen Aufklärung“

Die bislang in den §§ 5 ff. G10 und in § 19 BNDG geregelte „strategische Fernmeldeüberwachung“ soll als „strategische Aufklärung“ in den §§ 31 ff. BNDG-E neu geregelt werden. Die „Vorgaben für die strategische Aufklärung“ (§ 31 BNDG-E) orientieren sich ersichtlich an § 19 BNDG. Dies überrascht, weil die Eingriffsschwellen entfallen sollen, die bislang im Bereich „Inland-Ausland“ (§ 5 ff. G10) gelten:

Volumengrenze ohne reale Wirkung

§ 10 Abs. 4 Satz 3 G10 beschränkt die Ausleitung von Telekommunikationsverkehren auf maximal 20 Prozent „der auf diesen Übertragungswegen zur Verfügung stehenden Übertragungskapazität“. § 31 Abs. 3 Satz 2 Nr. 2 BNDG-E erweitert die Befugnis auf bis zu „15 Prozent des Datenvolumens, welches in allen Telekommunikationsnetzen übertragen werden kann“. Zunächst erzeugt die Norm Rechtsunklarheit durch den Begriff “aller Telekommunikationsnetze.” In ihrer weitesten Auslegung würde sie es dem Dienst ermöglichen, 15 Prozent der weltweiten Kommunikation abzufangen - mitnichten eine Begrenzung weder der bestehenden Rechtslage, noch der praktischen Arbeit des

Bundesnachrichtendienstes. Auch auf einzelne Übertragungswege gemünzt verdeutlicht folgendes Beispiel wie weitreichend die Regelung gefasst ist: Die Portkapazität des DE-CIX Knoten in Frankfurt beträgt aktuell 200 Terabit pro Sekunde, während in der Spitze in den vergangenen fünf Jahren 19,64 Terabit pro Sekunde übertragen wurden.[1] Der entscheidende Punkt liegt in der Bezugsgröße: Die Grenze bemisst sich nicht am tatsächlich übertragenen Datenverkehr, sondern an dem Volumen, das übertragen werden „kann“, also an der theoretisch verfügbaren Kapazität. Da die reale Auslastung evident und regelmäßig weit unterhalb dieser Kapazität liegt, kann eine an ihr bemessene Quote den vollständigen oder nahezu vollständigen Datenverkehr eines Übertragungswegs erfassen. Selbst wenn mit einem kontinuierlichen Wachstum des Datenverkehrs zu rechnen ist, grenzt die gesetzliche Beschränkung den Zugriff daher praktisch nicht ein. Sie ist der Sache nach keine Begrenzung, sondern eine Rechengröße ohne einschränkende Wirkung.

Löschpflicht als Speicherbefugnis

§ 66 Abs. 1 Satz 1 BNDG-E ist als Löschpflicht formuliert: Inhaltsdaten sind spätestens sechs Monate nach ihrer Erhebung zu löschen. Der Sache nach handelt es sich um eine Speicherbefugnis. Die Gesetzesbegründung stellt dies ausdrücklich klar (S. 474). Der Bundesnachrichtendienst kann Inhaltsdaten künftig zunächst speichern und erst später einsehen. Bislang war die Einsichtnahme unmittelbar an die Erhebung gekoppelt. Die Begründung führt zudem aus, dass der Bundesnachrichtendienst während dieser sechs Monate Suchbegriffe, die er erst nachträglich gewonnen hat, auf den gespeicherten Bestand anwenden darf. Kommunikation, die im Zeitpunkt ihrer Erhebung keinen Anlass zur Einsichtnahme bot, kann damit nach Kriterien durchsucht werden, die zu diesem Zeitpunkt noch nicht existierten. Für journalistische Vertraulichkeitsbeziehungen bedeutet das eine erhebliche Ausweitung des Risikos. Der Schutz einer Kommunikation entscheidet sich nicht mehr im Moment ihrer Erhebung, sondern bleibt für sechs Monate revidierbar. Hinzu kommt, dass dieser Datenbestand die Grundlage für die automatisierte, profilbildende Auswertung bildet, die bereits oben kritisiert wurde.

Wegfall des Suchbegriffverbots

§ 5 Abs. 2 G10 regelt die Suchbegriffe, mit denen der BND den Datenverkehr filtern darf, und untersagt unter anderem Identifizierungsmerkmale, die zu einer gezielten Überwachung einzelner Personen führen (§ 5 Abs. 2 Satz 2 Nr. 1 G10). Nach § 33 Abs. 3 BNDG-E sollen diese Einschränkungen weitgehend entfallen. Der BND soll bei der Auswahl von Suchbegriffen nur noch pauschal an den Verhältnismäßigkeitsgrundsatz gebunden sein. Für Journalistinnen und Journalisten im Ausland öffnet dies ein erhebliches Risiko: Ihre E-Mail-Adressen, Telefonnummern oder Messenger-Kennungen könnten grundsätzlich als Suchbegriffe verwendet werden, um ihre Kommunikation mit Quellen gezielt herauszufiltern – etwas, das der bisherige § 5 Abs. 2 G-10 kategorisch ausschloss.

Unter den in § 34 Abs. 2 BNDG-E geregelten Voraussetzungen soll eine gezielte Überwachung sogar bei „qualifiziertem Inlandsbezug“ zulässig sein. Die Verwendung personenbezogener Suchbegriffe soll ausnahmsweise zulässig sein, unter anderem wenn dies „zur Abwehr einer erheblichen Gefahr für ein besonders gewichtiges Rechtsgut" erforderlich ist. Wie bereits an anderer Stelle ausgeführt, handelt es sich hierbei um einen

[1] Frankfurt traffic statistics: https://www.de-cix.net/en/locations/frankfurt/statistics (zuletzt abgerufen am 11.07.2026)

denkbar unscharfen Maßstab, dessen Anwendung im Wesentlichen im Beurteilungsspielraum des BND selbst liegt. Der besondere Schutz, den das Inlandsbezug-Kriterium eigentlich vermitteln soll, wird damit an entscheidender Stelle wieder durchbrochen.

Entgrenzte Erkenntniszwecke

Schließlich entfällt auch die bislang in § 5 Abs. 1 Satz 2 G-10 enthaltene abschließende Aufzählung legitimer Erkenntniszwecke. An ihre Stelle tritt die denkbar weite Formel, wonach strategische Aufklärungsmaßnahmen lediglich „zur nachrichtendienstlichen Auslandsaufklärung erforderlich" sein müssen (§§ 32 Abs. 1 und 33 Abs. 1 BNDG-E). Für die journalistische Arbeit ist das bedeutsam, weil gerade investigative Recherchen zu Themen wie Rüstungsexporten, organisierter Kriminalität oder in Kriegs- und Konfliktsituationen inhaltlich in unmittelbarer Nähe zu klassischen Aufklärungsinteressen des BND liegen.

Wo bislang mehrere ineinandergreifende Schutzmechanismen die strategische Überwachung von Auslandskommunikation begrenzten, verbleibt künftig im Wesentlichen der Verhältnismäßigkeitsgrundsatz als einzige materielle Schranke: eine Abwägungsformel, die der BND im Kern selbst ausfüllt. In Kombination mit den bereits dargestellten Schwächen des § 22 BNDG-E beim Schutz journalistischer Vertraulichkeitsbeziehungen entsteht so ein Gesamtbild, in dem der Austausch mit Quellen im Ausland strukturell einem erheblich größeren Überwachungsrisiko ausgesetzt wird als bisher.

4. Zum Unabhängigen Kontrollrat

Für die Kontrolle der Nachrichtendienste sind derzeit die G10-Kommission, die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) und der Unabhängige Kontrollrat zuständig. Dies soll sich ändern. Alle Kontrollbefugnisse sollen beim Unabhängigen Kontrollrat zusammengefasst werden.

Ein fehlender Anwalt der Betroffenen

Der Kontrollrat soll weiterhin aus zwei Kontrollorganen bestehen – dem „gerichtsähnlichen Kontrollorgan“ und einem „administrativen Kontrollorgan“ (§ 5 UKRatG-E). Dem „gerichtsähnlichen Kontrollorgan“ fehlt es indes schon deshalb an „Gerichtsähnlichkeit“, weil kein kontradiktorisches Verfahren vorgesehen ist. Das „Kontrollorgan“ befasst sich mit Anträgen der Nachrichtendienste (§ 27 Abs. 2 und § 29 Abs. 2 UKRatG-E), einen „Anwalt der Betroffenen“ sieht der Gesetzesentwurf jedoch nicht vor, sodass es an einem Gegengewicht fehlt, das nach dem verfassungsrechtlichen Grundsatz der Waffengleichheit (Art. 103 Abs. 1 GG) geboten ist. Bürgerinnen und Bürger haben nach § 38 UKRatG-E zwar ein Petitionsrecht, wenn sie der Meinung sind, von einem Nachrichtendienst in eigenen Rechten verletzt worden zu sein. Der Kontrollrat ist jedoch lediglich verpflichtet, eine solche Petition zu „prüfen“, ein Beschwerderecht des Bürgers oder eine Verpflichtung des Kontrollrats zum Einschreiten gegen Rechtsverletzungen sieht das Gesetz nicht vor.

Beanstandung ohne Zähne, Anweisung ohne Sanktion

Auch dort, wo das administrative Kontrollorgan tatsächlich einen Verstoß feststellt, bleibt sein Instrumentarium stumpf. Bei einem einfachen Verstoß sieht § 33 UKRatG-E lediglich vor, dass der Unabhängige Kontrollrat diesen gegenüber der zuständigen Aufsichtsbehörde – regelmäßig also dem Bundeskanzleramt oder dem jeweiligen Fachministerium, die den

betroffenen Dienst selbst beaufsichtigen – „beanstanden" und um eine Stellungnahme bitten kann. Eine Pflicht zur Abhilfe, geschweige denn eine Möglichkeit, die beanstandete Maßnahme zu stoppen oder rückgängig zu machen, ist damit nicht verbunden; es bleibt bei einer möglicherweise folgenlosen Mitteilung unter Aufsichtsbehörden. Selbst der „qualifizierte Verstoß" nach § 34 UKRatG-E – beschränkt auf die engen Fälle einer verletzten Vorab- oder Einzelfallkontrolle, missachteter Maßgaben des gerichtsähnlichen Organs oder unzulässiger Weiterverarbeitung – führt lediglich zu einer „Anweisung" des Senats, die der betroffene Dienst innerhalb einer gesetzten oder unverzüglichen Frist umzusetzen hat. Kommt der Dienst dieser Anweisung nicht nach, sieht das Gesetz keinerlei Sanktion, kein Zwangsmittel und keine gerichtliche Durchsetzung vor – die einzige Konsequenz ist die Unterrichtung des Parlamentarischen Kontrollgremiums. Ob eine solche bloße Unterrichtung das strukturelle Durchsetzungsdefizit tatsächlich auffängt, erscheint fraglich: Das PKGr tagt nichtöffentlich, ist selbst zur Geheimhaltung verpflichtet und verfügt über keine eigenen exekutiven Zwangsbefugnisse gegenüber den Diensten – es kann politischen Druck erzeugen, aber ebenso wenig wie der Kontrollrat selbst eine rechtswidrige Maßnahme unmittelbar beenden. Für Journalistinnen und Journalisten, deren erfasste Kommunikation Gegenstand eines festgestellten, aber vom Dienst ignorierten Verstoßes ist, bedeutet dies: Selbst eine erfolgreiche Beanstandung durch die eigens geschaffene Kontrollinstanz verschafft ihnen keinerlei verbindlichen Schutz, solange der betroffene Dienst schlicht untätig bleibt.

Hält die Kontrolle mit den erweiterten Zuständigkeiten Schritt?

Trotz der erheblich erweiterten Kontrollbefugnisse, die sich nicht mehr – wie bislang – ausschließlich auf den BND, sondern auf alle Nachrichtendienste erstrecken sollen und die zudem auch die bislang bei der BfDI angesiedelte Datenschutzaufsicht umfassen soll, soll das „gerichtsähnliche Kontrollorgan“ aus lediglich 8 (statt bislang 6) Mitgliedern bestehen (§ 14 UKRatG-E). Die Zuständigkeit soll sich zudem beschränken auf „gesetzliche bestimmte“ Maßnahmen bzw. Fälle (§ 2 Abs. 2 Nr. 1 UKRatG-E). Sucht man in den beiden Gesetzen (BVerfSchG-E und BND-E) nach „gesetzlich bestimmten“ Zuständigkeiten des Kontrollorgans, findet man nicht viel. So soll dem BND beispielsweise der Einsatz von Trojanern in vielen Fällen ohne eine „Vorabkontrolle“ erlaubt sein (§ 97 Abs. 1 Nr. 14 i.V.m. § 37 Abs. 1 BNDG-E).

Zur „administrativen Kontrolle“ findet man im UKRatG-E ebenfalls nur wenig, obwohl die „administrative Kontrolle“ unter anderem Ersatz für die Kontrolle durch die Bundesdatenschutzbeauftragte sein soll. Überraschendes müssen die Dienste jedenfalls nicht befürchten, denn die „administrative Kontrolle“ (§ 32 UKRatG-E) soll eingehegt werden durch ein „Prüfprogramm“, das das „gerichtsähnliche Kontrollorgan“ nach vorheriger Anhörung der Nachrichtendienste „für einen Zeitraum von bis zu 24 Monaten“ beschließt (§ 26 UKRatG-E). Wenn beispielsweise die strategische Überwachung in einem solchen „Prüfprogramm“ einmal nicht enthalten sollte, weil andere Schwerpunkte festgesetzt worden sind, ist dieser gesamte Überwachungskomplex keiner „administrativen Kontrolle“ entzogen. Etwaige Datenschutzverstöße bleiben unbemerkt und sanktionslos.

Zur personellen und sachlichen Ausstattung des „administrativen Kontrollorgans" enthält der UKRatG-E selbst keine verbindlichen Vorgaben. Die Gesetzesbegründung (S. 231) beziffert den erwarteten Bedarf zwar konkret: Für den gesamten Unabhängigen Kontrollrat werden lediglich 37 Planstellen veranschlagt (zehn für administrative Verwaltungstätigkeiten und 27 für die gerichtsähnliche und administrative Rechtskontrolle zusammen). Jährlicher

Kostenpunkt: 8,86 Millionen Euro. Es erscheint zweifelhaft, ob eine derart knapp bemessene Personaldecke dem tatsächlichen Aufgabenzuwachs gerecht werden kann: Der Kontrollrat soll künftig nicht mehr nur den BND, sondern sämtliche Nachrichtendienste kontrollieren, zugleich die bislang bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit angesiedelte datenschutzrechtliche Aufsicht vollständig übernehmen und darüber hinaus neue komplexe technische Sachverhalte bewältigen, wie die Kontrolle KI-gestützter Auswertungssysteme. Es fehlt jedoch an einer gesetzlichen Absicherung des notwendigen technischen Sachverstands: Weder wird eine Mindestzahl an IT-affinen oder technisch spezialisierten Fachkräften vorgeschrieben, noch werden Anforderungen an eine kontinuierliche technische Fortbildung der Mitglieder normiert. Angesichts dessen, dass allein für die IT-Infrastrukturanpassung beim BND selbst einmalig 40 Millionen und jährlich rund 15 Millionen Euro veranschlagt wird, und sich der Aufwand beim BfV auf 94 Millionen respektive 269 Millionen Euro jährlich summiert, drängt sich die Frage auf, ob ein mit vergleichsweise geringen Mitteln ausgestattetes Kontrollorgan technisch überhaupt in der Lage sein wird, mit der fortschreitenden Digitalisierung und Automatisierung nachrichtendienstlicher Datenverarbeitung Schritt zu halten – und ob die bislang bei der BfDI gebündelte datenschutzrechtliche und technische Fachexpertise beim Übergang auf den Kontrollrat tatsächlich in vergleichbarer Tiefe erhalten bleibt.

Anders als die Bundesdatenschutzbeauftragte soll der Kontrollrat auch nicht zu einem jährlichen Tätigkeitsbericht verpflichtet werden. § 36 UKRatG-E sieht lediglich einen nicht näher spezifizierten „öffentlichen Bericht“ vor, der „erstmals für den Zeitraum der Kalenderjahre 2028 bis 2030…in abstrakter Form“ erstellt werden soll. Praktisch bedeutet das, dass mit dem ersten Prüfbericht erst in fünf Jahren zu rechnen ist.

Journalistinnen und Journalisten als externe Kontrollinstanz

Das Kontrolldefizit wird zusätzlich verschärft durch die vorgesehene Einschränkung des Informationsfreiheitsgesetzes. Danach werden nicht nur, wie bisher schon für die Nachrichtendienste selbst, alle Kontrollinstanzen in die Bereichsausnahme des § 3 Nr. 8 IFG aufgenommen, so dass Auskunftsansprüche gegenüber den Kontrollinstanzen selbst grundsätzlich ausgeschlossen sind. Mit der neu eingeführten Nr. 9 geht der Entwurf noch weiter: Erfasst wird jede Information, die „Vorgänge oder Tätigkeiten" der Nachrichtendienste betrifft, unabhängig davon, bei welcher Bundesbehörde sie vorliegt. Die externe Kontrolle der Kontrolleure bleibt so faktisch außerhalb der Reichweite der Öffentlichkeit.

Fazit

Diese strukturellen Schwächen des Unabhängigen Kontrollrats wiegen für den journalistischen Quellenschutz besonders schwer, weil sie ausgerechnet jene Instanz betreffen, die die an anderer Stelle beschriebenen materiell-rechtlichen Defizite, wie zum Beispiel die weit gefassten Ausnahmen bei Vertraulichkeitsbeziehungen nach § 22 BNDG-E oder die entgrenzte strategische Aufklärung nach §§ 31 ff. BNDG-E, auffangen und korrigieren müsste. Fehlt es an einem „Anwalt der Betroffenen" im gerichtsähnlichen Verfahren, werden die Interessen überwachter Journalistinnen und Journalisten von niemandem vertreten, wenn der BND etwa die Genehmigung einer Maßnahme gegen einen Medienschaffenden beantragt. Dass der Einsatz von Staatstrojanern in vielen Fällen ganz ohne Vorabkontrolle erfolgen darf, betrifft gerade jene besonders eingriffsintensive Maßnahme, die investigativ tätige Journalistinnen und Journalisten und ihre digitalen Kommunikationswege am unmittelbarsten bedroht. Und wenn die administrative Kontrolle

von einem Prüfprogramm abhängt, das die strategische Überwachung, das zentrale nachrichtendienstliche Instrument des BND, schlicht aussparen kann, bliebe selbst eine systematische, rechtswidrige Erfassung journalistischer Quellen möglicherweise über Jahre hinweg unentdeckt.

Schluss

Reporter ohne Grenzen fordert die Gesetzgeberin auf, die notwendige und grundsätzlich zu begrüßende Reform der Nachrichtendienste zu nutzen, um den Schutz von Journalistinnen und Journalisten und ihren Quellen zu stärken statt zu schwächen.

Bei einer Gesamtbetrachtung der in dieser Stellungnahme dargelegten Kritikpunkte zeigt sich ein durchgängiges Muster: In nahezu jedem für Journalistinnen und Journalisten relevanten Regelungsbereich senkt der Entwurf das bisherige Schutzniveau ab, anstatt es, wie es die ohnehin gebotene Zusammenführung von BND-Gesetz und G-10-Gesetz nahegelegt hätte, auf den jeweils höheren Standard anzuheben. Beim Schutz journalistischer Vertraulichkeitsbeziehungen wird die bislang für die Ausland-Inland-Kommunikation geltende, an eine konkrete Straftatbeteiligung geknüpfte höhere Schwelle des G-10-Gesetzes durch einen weiten Zusammenhangsbegriff ersetzt und damit auf das niedrigere Niveau der bisherigen Ausland-Ausland-Kommunikation abgesenkt; das strukturell verwandte § 32 BVerfSchG-E wiederum entwertet die frühere Verhältnismäßigkeitsprüfung des § 3b Abs. 2 G-10 zu einer bloßen Evidenzkontrolle. Beim Einsatz staatlicher Trojaner entfällt für dienstlich genutzte Geräte jede eigenständige Verhältnismäßigkeitsprüfung, jede unabhängige Vorabkontrolle und jede Mitteilungspflicht. Bei der strategischen Aufklärung fallen mit der Volumengrenze, dem Suchbegriffsverbot und dem abschließenden Zweckkatalog gleich drei tragende Schutzmechanismen des bisherigen G-10-Regimes weg, sodass an ihre Stelle im Wesentlichen nur noch eine vom BND selbst auszufüllende Verhältnismäßigkeitsklausel tritt. Und selbst dort, wo der Entwurf neue Kontrollstrukturen schafft, bleibt der Unabhängige Kontrollrat strukturell zu schwach, um diese materiellen Absenkungen aufzufangen. In der Summe handelt es sich damit nicht um vereinzelte, punktuelle Lücken, sondern um eine systematische Absenkung des Schutzniveaus für Journalistinnen und Journalisten entlang der gesamten Eingriffskette – von der Datenerhebung über die Auswertung bis zur Kontrolle –, die in ihrer Kumulation den verfassungsrechtlich gebotenen Schutz der Pressefreiheit und des Quellenschutzes ernsthaft gefährdet.

Dass ein wirksamer Schutz von Medienschaffenden mit der Aufklärungsfähigkeit der Nachrichtendienste vereinbar ist, zeigen die genannten Beispiele aus Frankreich und den Niederlanden. Beide sichern den Schutz nicht nur materiell-rechtlich, sondern auch verfahrensrechtlich ab, und beide Elemente ließen sich in die im Entwurf ohnehin vorgesehene Kontrollarchitektur des Unabhängigen Kontrollrats einfügen, ohne deren Grundstruktur zu verändern.

Im Einzelnen fordert Reporter ohne Grenzen:

1. ein hinreichendes Schutzniveau für Journalistinnen und Journalisten in den § 22 BNDG-E und § 32 BVerfSchG-E zu verankern

2. den Schutz von Vertraulichkeitsbeziehungen ausdrücklich auf die automatisierte, profilbildende Auswertung (§ 37 BVerfSchG-E; §§ 52 ff. BNDG-E) zu erstrecken und lernende Analyseverfahren einer begleitenden, wiederkehrenden Kontrolle zu unterwerfen;
3. für den Einsatz von Trojanern nach § 37 Abs. 1 BNDG-E eine eigenständige Verhältnismäßigkeitsprüfung, eine verbindliche unabhängige Vorabkontrolle durch den Unabhängigen Kontrollrat sowie eine Mitteilungspflicht einzuführen und damit den Anforderungen des Art. 4 der Verordnung (EU) 2024/1083 Rechnung zu tragen, der den Einsatz von Überwachungssoftware gegen Medienschaffende grundsätzlich untersagt; zudem ist ein wirksames Schwachstellenmanagement beim BSI sicherzustellen, das dem Interessenausgleich zwischen der Cybersicherheit der Allgemeinheit und nachrichtendienstlicher Aufklärung Rechnung trägt;
4. bei der strategischen Aufklärung eine reale Volumengrenze, die Streichung der Speicherung von Inhaltsdaten, ein Verbot personenbezogener Suchbegriffe sowie einen abschließenden Zweckkatalog nach dem Vorbild des bisherigen G-10-Gesetzes wiedereinzuführen;
5. den Unabhängigen Kontrollrat durch einen Anwalt der Betroffenen, durchsetzbare Beanstandungsbefugnisse, eine verbindliche jährliche Berichtspflicht und eine angemessene personelle Ausstattung zu einer tatsächlich wirksamen Kontrollinstanz auszubauen; für Maßnahmen, die absehbar journalistische Kommunikation erfassen, ist nach dem Vorbild des französischen und niederländischen Rechts eine gesonderte, berufsspezifische Vorabkontrolle vorzusehen; sowie die Einschränkungen des Informationsfreiheitsgesetzes zurückzunehmen, damit auch die externe, publizistische Kontrolle der Nachrichtendienste erhalten bleibt.

Reporter ohne Grenzen erkennt an, dass die Nachrichtendienste in einer veränderten Bedrohungslage handlungsfähig bleiben müssen. Wer ihre Befugnisse erweitert, muss aber auch die Kontrolle erweitern. Genau das unterlässt der Entwurf. Er verschiebt das Verhältnis von Eingriff und Kontrolle einseitig zulasten des Quellenschutzes, und er tut dies zu einem Zeitpunkt, zu dem der Europäische Gerichtshof für Menschenrechte der Bundesregierung bereits grundsätzliche Fragen zu genau diesen Befugnissen vorgelegt hat. Diese Fragen proaktiv zu beantworten, wäre die Aufgabe dieser Reform gewesen. Der Entwurf verpasst sie. Frankreich und die Niederlande zeigen, dass sich wirksame Auslandsaufklärung und ein belastbarer Quellenschutz nicht ausschließen. Reporter ohne Grenzen wird darauf bestehen, dass dieser Nachweis auch im deutschen Recht erbracht wird.

Wir stehen für den weiteren Gesetzgebungsprozess als Gesprächspartnerin zur Verfügung und bitten um Berücksichtigung unserer Anmerkungen im weiteren Gesetzgebungsverfahren.