Schaller, Christian

Research Report

Kommunikationsüberwachung durch den Bundesnachrichtendienst: Rechtlicher Rahmen und Regelungsbedarf

SWP-Studie, No. S 7/2016

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Schaller, Christian (2016) : Kommunikationsüberwachung durch den Bundesnachrichtendienst: Rechtlicher Rahmen und Regelungsbedarf, SWP-Studie, No. S 7/2016, Stiftung Wissenschaft und Politik (SWP), Berlin

This Version is available at:
https://hdl.handle.net/10419/252896

SWP-Studie
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale
Politik und Sicherheit

Christian Schaller

Kommunikations-überwachung durch den Bundesnachrichtendienst

Rechtlicher Rahmen und Regelungsbedarf

S 7
April 2016
Berlin

SWP-Studien unterliegen einem Begutachtungsverfahren durch Fachkolleginnen und -kollegen und durch die Institutsleitung *(peer review)*. Sie geben die Auffassung der Autoren und Autorinnen wieder.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6372

Inhalt

Dr. iur. Christian Schaller ist stellvertretender Leiter der Forschungsgruppe Globale Fragen.

Kommunikationsüberwachung durch den Bundesnachrichtendienst
Rechtlicher Rahmen und Regelungsbedarf

Die NSA-Affäre mit ihren Deutschlandbezügen wirft schwierige rechtliche Fragen auf. Problematisch ist vor allem die anlasslose, globale und massenhafte Überwachung elektronischer Kommunikation. Solche Aktivitäten sind mit den internationalen Normen zum Schutz der Menschenrechte kaum zu vereinbaren; und sie sind geeignet, außenpolitische Beziehungen zwischen Partnerstaaten empfindlich zu stören. Ernsthafte Kritik an den Aktivitäten ausländischer Nachrichtendienste lässt sich jedoch nur dann glaubhaft formulieren, wenn die eigene Praxis bestimmten Standards entspricht.

Die Bundesrepublik Deutschland tritt auf internationaler Ebene traditionell für liberale Werte ein, die die freiheitliche demokratische Grundordnung des Grundgesetzes ebenso prägen wie das Vertragswerk der Europäischen Union. Dazu zählen auch die Menschenrechte und die Idee von der Herrschaft des Rechts (»Rule of Law«). Im Rahmen der Vereinten Nationen engagiert sich Deutschland daher in besonderem Maße für den Schutz der Privatsphäre im digitalen Zeitalter (»the right to privacy in the digital age«). In den dazu von der UN-Generalversammlung verabschiedeten Resolutionen, die auf eine brasilianisch-deutsche Initiative zurückgehen, heißt es unter anderem, dass die Überwachung digitaler Kommunikation mit internationalen Menschenrechtsverpflichtungen vereinbar sein und auf Basis gesetzlicher Vorschriften erfolgen müsse, die öffentlich zugänglich, klar, präzise, umfassend und nicht diskriminierend sind. Dementsprechend sind die Staaten nach der Resolution aufgerufen, ihre eigenen Verfahren, Praktiken und gesetzlichen Vorgaben zu überprüfen (UN-Generalversammlung, Resolution 69/166 vom 18.12.2014).

Die vorliegende Studie untersucht, welche rechtlichen Anforderungen das Grundgesetz an die Kommunikationsüberwachung durch den Bundesnachrichtendienst (BND) stellt und wie diese Anforderungen legislativ umgesetzt worden sind. In den Fällen, in denen der BND elektronische Kommunikation überwacht, können vor allem das Fernmeldegeheimnis, das Grundrecht auf informationelle Selbstbestimmung sowie das Grundrecht auf Gewährleistung der

Vertraulichkeit und Integrität informationstechnischer Systeme betroffen sein. Das Bundesverfassungsgericht hat den Schutz dieser Grundrechte engmaschig ausgestaltet. Von zentraler Bedeutung ist unter anderem, ob und in welchem Umfang auch ausländische Personen im Ausland durch diese Grundrechte gegenüber der deutschen öffentlichen Gewalt geschützt sind. Davon hängt maßgeblich ab, welchen Bindungen der BND bei der Überwachung rein ausländischer Kommunikation unterliegt. Darüber hinaus geht es in der Studie auch darum, die rechtlichen Grenzen für einen Austausch personenbezogener Daten mit ausländischen Nachrichtendiensten auszuloten.

In vielerlei Hinsicht ergeben sich aus den Grundrechten strengere Maßstäbe als aus den völkerrechtlich verankerten Menschenrechten. Bei eingehender Analyse der aktuellen Gesetzeslage wird deutlich, dass gerade im Bereich der strategischen Telekommunikationsüberwachung Regelungsbedarf besteht. Ob der für die nachrichtendienstliche Auslandsüberwachung und für den Informationsaustausch mit ausländischen Diensten geltende Rechtsrahmen verändert werden muss, ist eine Frage, mit der sich auch der vom Deutschen Bundestag eingesetzte NSA-Untersuchungsausschuss beschäftigt.

In Anbetracht der wachsenden Bedrohung durch den internationalen Terrorismus ist es notwendig, dass der BND mit anderen Nachrichtendiensten effektiv kooperieren kann. Selbstverständlich ist das Interesse an einem funktionierenden Informationsaustausch mit der Forderung nach mehr Rechtssicherheit und einem besseren Schutz individueller Rechte in Einklang zu bringen, und selbstverständlich stellt dies eine große Herausforderung dar. Ausländische Nachrichtendienste verfügen nach nationalem Recht teilweise über größere Handlungsspielräume als der BND. Werden auf der Arbeitsebene Absprachen mit solchen Diensten getroffen, gilt es sicherzustellen, dass der BND seine grundrechtlichen und gesetzlichen Bindungen auch im Rahmen der Kooperation einhält. Der Vorteil solcher Absprachen – auch wenn sie rechtlich unverbindlich sind – besteht darin, dass sich die Kooperationspartner bis zu einem gewissen Grad auf die Einhaltung bestimmter Prinzipien verlassen können. Denn Gegenseitigkeitserwartungen spielen bei der nachrichtendienstlichen Zusammenarbeit eine wichtige Rolle. Auch in den Rechtsordnungen anderer Staaten gibt es Rechtsgarantien, die beispielsweise dem deutschen Fernmeldegeheimnis vergleichbar sind.

Die Hoffnung dürfte unbegründet sein, dass sich Staaten wie die USA oder Großbritannien völkerrechtlich verbindlichen Vereinbarungen zur Begrenzung der gegenseitigen Überwachung unterwerfen könnten. Möglicherweise lassen sich aber auf EU-Ebene gemeinsame Leitplanken für einen verbesserten Schutz elektronischer Kommunikation vor massenhafter Ausspähung schaffen. Welche Impulse hierbei von Deutschland ausgehen können, hängt unter anderem davon ab, ob es gelingt, die eigene nachrichtendienstliche Praxis an den hohen Standards des deutschen Grundrechtsschutzes auszurichten und dies glaubhaft zu vermitteln.

Grundbegriffe

Sinn und Zweck der nachrichtendienstlichen Aufklärung ist es, Informationen zu sammeln, aus denen sich – je nach Auftrag – außen- und sicherheitspolitisch relevante Erkenntnisse über das Ausland gewinnen lassen. Einen Teil ihrer Informationen beziehen Nachrichtendienste aus allgemein zugänglichen Quellen. Die Überwachung elektronischer Kommunikation zielt aber darauf ab, große Mengen vertraulicher Daten ohne Wissen der Betroffenen zu erheben. Im Prinzip kann jeder Kommunikationsvorgang, der elektronisch abläuft, mit technischen Mitteln überwacht werden. Dies betrifft das Telefonieren, das Versenden von Telefaxen und das Schreiben von SMS-Nachrichten und E-Mails ebenso wie das Aufrufen von Webseiten, Auftritte in sozialen Netzwerken oder die Nutzung anderer Online-Dienste. Im nachrichtendienstlichen Kontext wird die Überwachung solcher Aktivitäten unter der Bezeichnung »Communication Intelligence« (COMINT) zusammengefasst. Dem entspricht im deutschen Sprachgebrauch der Begriff der Fernmeldeaufklärung. Sie ist Teil der signalerfassenden Aufklärung (Signals Intelligence, SIGINT).

Grundsätzlich ist zwischen der gezielten Überwachung einzelner Personen und der strategischen Überwachung zu differenzieren. Die strategische Fernmeldeaufklärung richtet sich typischerweise auf bestimmte Staaten oder Krisenregionen. Dabei werden aus einer großen Menge von Telekommunikationsverbindungen mit Hilfe von Suchbegriffen (Selektoren) einzelne Verbindungen automatisiert erfasst, gespeichert und ausgewertet. Unterschieden wird zwischen formalen und inhaltlichen Suchbegriffen. Formale Suchbegriffe werden beispielsweise aus Telefonnummern gebildet, ebenso aus Gerätekennungen von Mobiltelefonen, aus Mobilfunk-Teilnehmerkennungen, E-Mail-Adressen und Adressen, die zur Internet-Telefonie verwendet werden. Ein Suchprofil beinhaltet regelmäßig auch die unterschiedlichen technischen Schreibweisen (Permutationen) solcher Adressen. Als inhaltliche Suchbegriffe kommen Wörter in Betracht, die zum Beispiel mit einem bestimmten Gefahrenbereich in Verbindung stehen. Inhaltliche Suchbegriffe müssen jedoch möglichst spezifisch sein. Andernfalls ist das Aufkommen irrelevanten Kommunikationsverkehrs sehr hoch. Daher werden solche Begriffe nur selten in Suchprofile eingestellt.[1]

In den Fällen, die den im März 2014 eingesetzten Untersuchungsausschuss des Deutschen Bundestages beschäftigen,[2] hat der BND in großem Umfang auch Selektoren »gesteuert«, die ihm im Rahmen einer Kooperation in seiner Außenstelle in Bad Aibling von der amerikanischen National Security Agency (NSA) zur Verfügung gestellt wurden. Je umfassender solche strategischen Überwachungsmaßnahmen sind, je länger sie andauern und je weniger sie auf einen konkreten Anlass zurückgehen, desto problematischer sind sie unter rechtlichen Gesichtspunkten. Über die Praxis der NSA und des britischen Nachrichtendienstes GCHQ wurde nach den Enthüllungen von Edward Snowden ausführlich berichtet.[3] Gegenwärtig beleuchtet der Untersuchungsausschuss des Bundestages unter anderem die Rolle des BND im Zusammenhang mit diesen Vorkommnissen.

Bei elektronischen Kommunikationsvorgängen entstehen Inhaltsdaten und Metadaten. Inhaltsdaten sind Daten, die von den Kommunikationsteilnehmern als Nachricht ausgetauscht werden, etwa der Inhalt eines Telefongesprächs, einer E-Mail oder eines Webformulars, ein Bild oder ein Video.[4] Bei Metadaten handelt es

1 Kurt Graulich, *Nachrichtendienstliche Fernmeldeaufklärung mit Selektoren in einer transnationalen Kooperation. Prüfung und Bewertung von NSA-Selektoren nach Maßgabe des Beweisbeschlusses BND-26*, Bericht (offene Vers.), Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, MAT A SV-11/2, zu A-Drs. 404, 23.10.2015, S. 24ff, <www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848> (Zugriff am 12.4.2016).

2 Antrag der Fraktionen CDU/CSU, SPD, Die Linke und Bündnis 90/Die Grünen auf Einsetzung eines Untersuchungsausschusses (BT-Drs. 18/843). Nähere Informationen unter <www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss> (Zugriff am 12.4.2016).

3 Siehe z.B. Glenn Greenwald, *Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen*, München 2014.

4 Michael Waidner, *Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 26. Juni 2014*, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, MAT A SV-1/2, zu A-Drs. 53, 26.6.2014, S. 15. Die schriftlichen Stellungnahmen der Sachverständigen sowie die Stenografischen Protokolle der Sitzungen, in denen die Sachverständigen

sich um Daten, die Informationen über den Kommunikationsvorgang als solchen enthalten. In der telekommunikationsrechtlichen Terminologie wird der Begriff »Verkehrsdaten« verwendet.[5] Im Falle eines Telefon- oder E-Mail-Verkehrs geben Metadaten unter anderem Auskunft über die Adressen der Kommunikationsteilnehmer, den in Anspruch genommenen Dienst, Beginn und Ende des Verkehrs sowie den Umfang der übertragenen Inhaltsdaten. Beim Aufrufen einer Webseite ergibt sich aus den Metadaten zum Beispiel die URL der jeweiligen Seite, die IP-Adresse des Nutzers, der Zeitpunkt des Abrufs und der Aufenthaltsort des Nutzers. Metadaten sind aufgrund ihrer Strukturierung relativ einfach maschinell zu verarbeiten.[6]

Die Erhebung von Metadaten ist für Nachrichtendienste vor allem deshalb interessant, weil sich daraus mit Hilfe von Algorithmen, die Verknüpfungen herstellen und Wahrscheinlichkeiten einbeziehen, Schlüsse auf soziale Beziehungen, Lebenssituationen, Interessen, Einstellungen und Kompetenzen von Personen ziehen lassen. Im Prinzip geht es darum, sehr große und schnell anwachsende Mengen von Inhaltsdaten und Metadaten aus einer Vielzahl von Quellen so schnell wie möglich zu erfassen, zu verarbeiten und miteinander in Beziehung zu setzen (»Big Data«). Auf diesem Wege lässt sich nach Mustern und Korrelationen suchen, so dass möglicherweise Zusammenhänge sichtbar werden, die vorher nicht bekannt waren.[7] Eines der gegenwärtig leistungsstärksten und prominentesten Programme, die von Nachrichtendiensten zur Analyse von Metadaten genutzt werden, ist X-Keyscore.[8]

Die Übertragung elektronischer Kommunikation erfolgt heute in erster Linie über Glasfaserkabel (»leitungsgebunden«) oder Satellit (»nichtleitungsgebunden«). Richtfunk spielt nur noch eine untergeordnete Rolle. Hinsichtlich der Übertragungsart ist zwischen Leitungsvermittlung und Paketvermittlung zu differenzieren. Bei der Leitungsvermittlung wird zwischen den Kommunikationsteilnehmern über Vermittlungsstationen für die Dauer der Übertragung eine direkte Leitung aufgebaut. Der heute gängige Standard ist die Paketvermittlung. Dabei erfolgt die Übertragung der Nachrichten fragmentiert. Dies bedeutet, dass die Daten einer Nachricht auf mehrere Pakete verteilt und später wieder zusammengesetzt werden. Die zentrale Infrastruktur für elektronische Kommunikation ist das Internet, das aus zahlreichen autonomen Teilnetzen besteht.[9] Die Übertragung von Daten innerhalb dieser Teilnetze und zwischen ihnen erfolgt nach einem einheitlichen Standard über Glasfaserkabel, Router und Knotenpunkte. Der Knotenpunkt mit dem weltweit größten Datendurchsatz ist derzeit das DE-CIX in Frankfurt am Main. Solche Knotenpunkte sind für eine Überwachung besonders geeignet, da hier auf sehr viele Verbindungen zugegriffen werden kann. Welchen Weg die Daten bei der paketvermittelten Kommunikation nehmen, legen die Betreiber der jeweiligen Teilnetze fest. Dabei sind vor allem Kosten und Kapazitäten ausschlaggebend. So werden Nachrichtenpakete nicht immer über den geographisch kürzesten Weg weitergeleitet, sondern häufig über größere globale Teilnetze.[10] Daher kann es beispielsweise sein, dass ein Telefonat oder E-Mail-Verkehr zwischen zwei Kommunikationsteilnehmern in Deutschland über Staaten abgewickelt wird, in denen andere gesetzliche Schranken und andere Zugriffsmöglichkeiten als in der Bundesrepublik bestehen. Die meisten Betreiber größerer Teilnetze haben ihren Sitz in den USA. Hinzu kommt, dass nur ein geringer Teil des Internet-Verkehrs verschlüsselt ist.[11]

öffentlich angehört wurden, sind auf der Website des Untersuchungsausschusses [wie Fn. 2] veröffentlicht.

5 § 3 Nr. 30 TKG definiert »Verkehrsdaten« als Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Siehe auch § 96 TKG.

6 Waidner, *Stellungnahme* [wie Fn. 4], S. 16. Siehe auch Sandro Gaycken, Sachverständigengutachten »IT-Infrastruktur« zur Anhörung des 1. Untersuchungsausschusses, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, MAT A SV-1/1, zu A-Drs. 53, 26.6.2014, S. 4.

7 Waidner, *Stellungnahme* [wie Fn. 4], S. 17ff.

8 Dazu Gaycken, *Sachverständigengutachten* [wie Fn. 6], S. 5.

9 Waidner, *Stellungnahme* [wie Fn. 4], S. 9ff.

10 Ebd., S. 11.

11 Ebd., S. 10.

Völkerrechtlicher Rahmen der Überwachung

Spionage gilt in der Staatenwelt seit jeher als legitimes Mittel, um Erkenntnisse zu gewinnen, die für die Lagebeurteilung und Entscheidungsfindung im politischen, militärischen und wirtschaftlichen Bereich relevant sein können. Dementsprechend üben die Staaten größte Zurückhaltung, wenn es darum geht, entsprechende Aktivitäten völkerrechtlich zu bewerten. Im internationalen Vertragsrecht existiert jedenfalls kein generelles Spionageverbot; und auch aus dem Völkergewohnheitsrecht lässt sich ein solches Verbot nicht ableiten. Lediglich in einigen Bereichen wie dem Diplomaten- und Konsularrecht, dem Truppenstationierungsrecht, dem Rüstungskontrollrecht, dem Seerecht oder dem Recht internationaler bewaffneter Konflikte finden sich vereinzelt Regelungen, die auf spionagerelevante Aktivitäten Bezug nehmen und bestimmte Sanktionen vorsehen. Außerdem stellen Übergriffe wie das illegale Eindringen ausländischer Agenten in fremdes Staatsgebiet oder unerlaubte Überflüge von Aufklärungsflugzeugen Verletzungen der Souveränität dar.[12] Umstritten ist, ob das virtuelle Einbrechen in Computersysteme oder Netzwerke, deren Server sich in einem fremden Hoheitsbereich befinden, als Souveränitätsverletzung oder gar als verbotene Intervention zu werten ist.[13] Da jeder Staat ein Interesse daran hat, sich möglichst effektiv vor Spionage zu schützen, enthalten die nationalen Rechtsordnungen durchgängig Vorschriften, die solche Handlungen unter Strafe stellen.

Die Überwachung elektronischer Kommunikation durch staatliche Nachrichtendienste, gerade wenn sie anlasslos und massenhaft erfolgt, ist jedoch unter menschenrechtlichen Gesichtspunkten äußerst problematisch. Bereits die Allgemeine Erklärung der Menschenrechte, die von der UN-Generalversammlung 1948 verabschiedet wurde und in weiten Teilen Völkergewohnheitsrecht widerspiegelt, garantiert in Artikel 12 den Schutz der Privatsphäre. Auf vertraglicher Ebene ist die Privatsphäre unter anderem durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) von 1950 und den Internationalen Pakt über bürgerliche und politische Rechte (Zivilpakt) von 1966 geschützt.

Gemäß Art. 8 Abs. 1 EMRK hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. Der Europäische Gerichtshof für Menschenrechte hat dieses Recht im Zusammenhang mit nachrichtendienstlichen Überwachungsmaßnahmen mehrfach konkretisiert.[14] Ein staatlicher Eingriff ist nach Art. 8 Abs. 2 zulässig, sofern er gesetzlich geregelt und »in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer«. Eine gesetzliche Ermächtigung zur geheimen Überwachung von Bürgerinnen und Bürgern ist nach Ansicht des Europäischen Gerichtshofs für Menschenrechte jedoch nur tolerierbar, soweit sie zum Schutz demokratischer Institutionen unbedingt erforderlich ist.[15] In jedem Fall müssen angemessene und wirksame Garantien gegen einen Missbrauch solcher Befugnisse vorgesehen sein.[16]

Gemäß Art. 1 EMRK sichern die Vertragsparteien die in der Konvention enthaltenen Rechte aber nur Personen zu, die ihrer Hoheitsgewalt unterstehen (»everyone within their jurisdiction«). Ein Staat, der Personen gleich welcher Staatsangehörigkeit auf seinem eigenen Territorium überwacht, übt Hoheitsgewalt aus und ist dabei in jedem Fall an Art. 8 EMRK

12 Simon Chesterman, »Secret Intelligence«, in: Rüdiger Wolfrum (Hg.), *Max Planck Encyclopedia of Public International Law*, Online Edition, Oxford 2015, <http://opil.ouplaw.com/home/epil> (Zugriff am 12.4.2016).

13 Dazu Christian Schaller, *Internationale Sicherheit und Völkerrecht im Cyberspace. Für klarere Regeln und mehr Verantwortung*, Berlin: Stiftung Wissenschaft und Politik, Oktober 2014 (SWP-Studie 18/2014), S. 12.

14 European Court of Human Rights, *Klass and others v. Germany*, Application no. 5029/71, Judgment, 6.9.1978; *Rotaru v. Romania*, Application no. 28341/95, Judgment, 4.5.2000; *Weber and Saravia v. Germany*, Application no. 54934/00, Decision as to the Admissibility, 29.6.2006; *Liberty and others v. The United Kingdom*, Application no. 58243/00, Judgment, 1.7.2008; *Kennedy v. The United Kingdom*, Application no. 26839/05, Judgment, 18.5.2010.

15 *Klass and others v. Germany* [wie Fn. 14], Abs. 42; *Rotaru v. Romania* [wie Fn. 14], Abs. 47.

16 *Klass and others v. Germany* [wie Fn. 14], Abs. 50; *Weber and Saravia v. Germany* [wie Fn. 14], Abs. 106.

gebunden. Schwieriger zu beantworten ist die Frage, ob diese Bindung auch dann besteht, wenn Personen im Ausland ausgespäht werden. Nach der nicht einheitlichen Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte übt ein Staat außerhalb seines Territoriums Hoheitsgewalt aus, wenn er entweder effektive Kontrolle über ein Gebiet oder (unter gewissen Bedingungen) über eine Person hat. Der bisherigen Rechtsprechung liegt jedoch insgesamt ein physisches Verständnis von Kontrolle zugrunde, das sich nicht ohne weiteres auf die Überwachung digitaler Kommunikation übertragen lässt. In der Literatur wird daher zum Teil versucht, den Begriff der Kontrolle im Cyberkontext so weit zu fassen, dass bestimmte Formen virtueller Kontrolle darunter fallen.[17] Zudem stellt auch die Übermittlung privater Daten und deren weitere Nutzung durch Dritte einen Eingriff in Art. 8 EMRK dar.[18] Dementsprechend wird von wissenschaftlicher Seite zum Beispiel argumentiert, dass eine außerhalb des eigenen Staatsgebiets stattfindende Überwachungsmaßnahme, die nur allgemein den Internetverkehr kontrolliere, vielleicht nicht in jedem Einzelfall als Ausübung von Hoheitsgewalt angesehen werden könne; der Charakter der Maßnahme wandle sich aber spätestens dann, wenn die Daten in Datenbanken auf dem eigenen Staatsgebiet gespeichert und weiterverarbeitet würden.[19] Viele der Fragen, die sich in Bezug auf Inhalt und Reichweite des menschenrechtlichen Schutzes vor staatlicher Ausspähung stellen, sind in ähnlicher Form auch im Rahmen der Grundrechtsprüfung nach deutschem Verfassungsrecht relevant. Weiter unten werden diese Fragen im Lichte der Grundrechte noch einmal ausführlicher behandelt.

Gemäß Art. 17 des Internationalen Zivilpaktes, dem auch die USA unterliegen, darf niemand willkürlichen oder rechtswidrigen Eingriffen in seine Privatheit, Familie, Wohnung oder Korrespondenz ausgesetzt werden. Die Staaten sind nicht nur selbst an dieses Verbot gebunden, sondern haben aktiv dafür Sorge zu tragen, dass Personen in ihrem Hoheitsbereich vor solchen Eingriffen durch andere Staaten sowie durch nichtstaatliche Akteure geschützt sind. Zu diesem Zweck müssen die Staaten Gesetze erlassen, die Art und Umfang zulässiger Eingriffe genau definieren.[20] Eine flächendeckende und verdachtsunabhängige Überwachung der elektronischen Kommunikation ist mit Art. 17 des Zivilpaktes jedenfalls nicht vereinbar.

Im April 2014 hat der für den Pakt zuständige UN-Menschenrechtsausschuss seine Bedenken gegen die Praxis der USA in einer Stellungnahme veröffentlicht.[21] Unter anderem empfahl der Ausschuss, dass alle Überwachungsaktivitäten, gleichgültig ob innerhalb oder außerhalb der USA, durch öffentlich zugängliche Gesetze präzise geregelt werden. Außerdem sollten nach Ansicht des Ausschusses effektive Vorkehrungen gegen Missbrauch getroffen, das bestehende Aufsichtssystem in den USA reformiert und betroffenen Personen in Missbrauchsfällen wirksamer Rechtsschutz gewährt werden. Auch für den Internationalen Zivilpakt stellt sich jedoch die Frage nach dem räumlichen Anwendungsbereich. Art. 2 Abs. 1 des Zivilpaktes sieht vor, dass jeder Vertragsstaat verpflichtet ist, die in dem Pakt anerkannten Rechte allen in seinem Gebiet befindlichen und seiner Hoheitsgewalt unterstehenden Personen (»all individuals within its territory and subject to its jurisdiction«) zu gewähren. Der UN-Menschenrechtsausschuss hat bereits 2004 klargestellt, dass die Verpflichtungen gegenüber allen Personen bestehen, die sich unter der Gewalt oder effektiven Kontrolle (»anyone within the power or effective control«) eines Vertragsstaates befinden. Unerheblich sei, ob sich die betreffende Person tatsächlich auf dem Territorium der jeweiligen Vertragspartei aufhalte.[22] Die Anwendbarkeit des Internatio-

17 Anne Peters, »Surveillance without Borders: The Unlawfulness of the NSA-Panopticon, Part II«, *EJIL: Talk!* (Blog of the European Journal of International Law), 4.11.2013, <www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/> (Zugriff am 12.4.2016). Ausführlich dazu Helmut Philipp Aust, »Spionage im Zeitalter von Big Data. Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht«, in: *Archiv des Völkerrechts*, 52 (2014), S. 375–406; Marko Milanovic, »Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age«, in: *Harvard International Law Journal*, 56 (2015) 1, S. 81–146.

18 *Weber and Saravia v. Germany* [wie Fn. 14], Abs. 79.

19 Helmut Philipp Aust, *Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014*, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, MAT A SV-4/1, zu A-Drs. 56, 28.5.2014, S. 13f.

20 Human Rights Committee, International Covenant on Civil and Political Rights, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, UN-Dok. A/43/40, Annex VI, 28.9.1988.

21 Human Rights Committee, International Covenant on Civil and Political Rights, *Concluding Observations on the Fourth Periodic Report of the United States of America*, UN-Dok. CCPR/C/USA/CO/4, 23.4.2014. Die vom 31.3.2015 datierende Antwort der US-Regierung auf die Empfehlungen des Menschenrechtsausschusses findet sich unter <www.state.gov/documents/organization/242228.pdf> (Zugriff am 12.4.2016).

22 Human Rights Committee, International Covenant on

nalen Zivilpaktes in Fällen, in denen ein Staat außerhalb seines eigenen Territoriums Hoheitsgewalt ausübt, wurde zudem auch vom Internationalen Gerichtshof bestätigt.[23] Zur juristischen Auslegung des Merkmals der effektiven Kontrolle im Cyberkontext kann auf die Ausführungen zu Art. 8 EMRK verwiesen werden (siehe S. 9f).

Bei den Ausspähaktionen durch die USA kommt hinzu, dass die überwachte Kommunikation – selbst wenn es sich um Personen in Deutschland und anderen europäischen Staaten handelt – im Regelfall über Unternehmen erfolgt, die in den USA registriert sind und deren Server amerikanischer Jurisdiktion unterstehen. Die USA (ebenso wie Israel) zeigen sich unbeeindruckt von der Rechtsmeinung des UN-Menschenrechtsausschusses und des Internationalen Gerichtshofs zur extraterritorialen Anwendbarkeit des Internationalen Zivilpaktes. Sie vertreten die Position, dass der Zivilpakt keinerlei extraterritoriale Bindung entfalte, sondern nur Personen innerhalb des eigenen Staatsgebiets schütze.[24] Derzeit ist nicht absehbar, wie diese grundlegenden juristischen Differenzen im transatlantischen Verhältnis überwunden werden könnten.

Bei den Vereinten Nationen jedoch hat der Schutz der Menschenrechte im digitalen Zeitalter während der vergangenen Jahre enorm an Bedeutung gewonnen. Insbesondere die Generalversammlung, der Menschenrechtsrat und der Hohe Kommissar für Menschenrechte haben sich dieses Themas angenommen. Ein wichtiger Impuls ging dabei von Deutschland und Brasilien aus. Im Zusammenhang mit der NSA-Affäre haben beide Staaten gemeinsam einen Resolutionsentwurf eingebracht, der sich mit dem Recht auf Privatheit im digitalen Zeitalter befasst. Er wurde im Dezember 2013 von der Generalversammlung angenommen.[25] In der Resolution wird betont, dass das unrechtmäßige oder willkürliche Überwachen und Abfangen von Kommunikation und das unrechtmäßige oder willkürliche Sammeln persönlicher Daten das Recht auf Privatheit sowie das Recht auf freie Meinungsäußerung verletzten. Ohne bestimmte Staaten zu verurteilen, bezieht sich die Resolution in erster Linie auf grenzüberschreitende und massenhafte Überwachungsmaßnahmen. Allgemein wird bekräftigt, dass die Rechte, die den Menschen »offline« zustehen, auch »online« zu schützen seien. Daher werden die Staaten unter anderem aufgefordert, ihre Überwachungspraxis und die zugrunde liegende Gesetzgebung im Lichte der einschlägigen Menschenrechtsverpflichtungen zu überprüfen und unabhängige nationale Aufsichtsmechanismen zu schaffen. Im Dezember 2014 wurde die Resolution mit einigen Erweiterungen erneut verabschiedet.[26]

Jenseits der menschenrechtlichen Dimension des Schutzes der Privatsphäre ist der Datenschutz auf völkerrechtlicher Ebene allerdings noch relativ unterentwickelt.[27] Ein universelles völkerrechtliches Datenschutzabkommen existiert nicht. Hervorzuheben ist aber, dass 1981 im Rahmen des Europarats eine Konvention verabschiedet wurde, die den Schutz individueller Rechte und Grundfreiheiten bei der automatischen Verarbeitung personenbezogener Daten gewährleisten soll.[28] Die Konvention steht auch jenen Staaten zum Beitritt offen, die nicht zu den Mitgliedern des Europarats zählen.[29] Ergänzt wird die Konvention durch ein Zusatzprotokoll von 2001, das unter anderem die Übermittlung personenbezogener Daten an Staaten und Organisationen regelt, die nicht Vertragsparteien sind.[30] Zudem finden sich spezielle Regelun-

Civil and Political Rights, *CCPR General Comment No. 31 [80]: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, UN-Dok. CCPR/C/21/Rev.1/Add.13, 26.5.2004, Abs. 10.

23 International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) (2004), ICJ Reports, S. 136–203 (178ff).

24 Siehe U.S. Department of State, *Fourth Periodic Report of the United States of America to the United Nations Committee on Human Rights Concerning the International Covenant on Civil and Political Rights*, Washington, D.C., 30.12.2011, Abs. 505, <www.state.gov/j/drl/rls/179781.htm> (Zugriff am 12.4.2016).

25 UN General Assembly, Resolution 68/167, *The Right to Privacy in the Digital Age*, 18.12.2013 (UN-Dok. A/RES/68/167, 21.1.2014).

26 UN General Assembly, *Resolution 69/166*, 18.12.2014 (UN-Dok. A/RES/69/166, 10.2.2015).

27 Dazu Stefan Talmon, *Sachverständigengutachten gemäß Beweisbeschluss SV-4*, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, MAT A SV-4/2, zu A-Drs. 56, 2.6.2014, S. 1ff. Zum unionsrechtlichen Datenschutz siehe auch Aust, *Stellungnahme* [wie Fn. 19], S. 20ff.

28 »Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten«, 28.1.1981, <www.coe.int/de/web/conventions/full-list/-/conventions/treaty/108> (Zugriff am 12.4.2016).

29 Bislang ist Uruguay der einzige Nichtmitgliedstaat, der dem Übereinkommen beigetreten ist. Zum aktuellen Stand der Ratifikationen und Beitritte siehe <www.coe.int/de/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=vjH2yzUi> (Zugriff am 12.4.2016).

30 »Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr«, 8.11.2001, <www.coe.int/de/

gen zum Schutz der Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen in der Europarat-Konvention gegen Computerkriminalität von 2001.[31] Erfasst werden unter anderem das Eindringen in fremde Systeme, das unbefugte Abfangen von Datenübermittlungen, die Manipulation von Computerdaten, das Sabotieren von Computersystemen sowie der Missbrauch (Herstellung, Verbreitung und Besitz) von Programmen und Zugangscodes, um solche Straftaten zu begehen.

web/conventions/full-list/-/conventions/treaty/181> (Zugriff am 12.4.2016).

31 »Übereinkommen über Computerkriminalität«, 23.11.2001, <www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185> (Zugriff am 12.4.2016).

Grundrechtliche Gewährleistungen zum Schutz vor Überwachung

Das deutsche Pendant zu den völkerrechtlichen Menschenrechten sind die im Grundgesetz (GG) der Bundesrepublik garantierten Grundrechte. Deren Inhalt und Reichweite werden durch das Bundesverfassungsgericht ständig konkretisiert und aktuellen Herausforderungen angepasst. Auch unter grundrechtlichen Gesichtspunkten wirft die Überwachung elektronischer Kommunikation erhebliche Probleme auf.

Das Fernmeldegeheimnis (Art. 10 GG)

Der Schutzbereich des Fernmeldegeheimnisses nach Art. 10 GG umfasst sowohl den Inhalt der individuellen Kommunikation als auch die näheren Umstände des Fernmeldevorgangs. Unerheblich sind Übermittlungsart und Ausdrucksform (Sprache oder sonstige Daten). Geschützt ist auch die Kommunikation mittels Internet. Spuren, die der Nutzer bei der digitalen Kommunikation in Form von Metadaten hinterlässt, sind ebenfalls vom Fernmeldegeheimnis erfasst. Keinen Unterschied macht es, ob der Kommunikationsinhalt privater, geschäftlicher oder politischer Art ist.[32]
Art. 10 GG gewährleistet jedoch nur die Vertraulichkeit des laufenden Kommunikationsvorgangs (sowohl auf der Übertragungsstrecke als auch am Endgerät). Nicht geschützt ist hingegen die Vertraulichkeit von Daten, die sich bereits im Herrschaftsbereich der Kommunikationsteilnehmer befinden, etwa wenn sie auf einer Computerfestplatte oder einer SIM-Karte in einem Mobiltelefon gespeichert sind. Der Schutz solcher Daten ergibt sich aus dem Recht auf informationelle Selbstbestimmung und dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie gegebenenfalls aus Art. 13 GG (Unverletzlichkeit der Wohnung). Anders verhält es sich mit E-Mails, die auf dem Mailserver des Providers und nicht im Herrschaftsbereich des Nutzers gespeichert sind. Insoweit greift der Schutz nach Art. 10 GG.[33]

Schon der erste Zugriff, mit dem sich die öffentliche Gewalt ohne Zustimmung der Kommunikationsteilnehmer Zugang zum Inhalt oder Kenntnis über die Umstände eines Kommunikationsvorgangs verschafft, stellt einen Eingriff in Art. 10 GG dar. Auch Anordnungen, mit denen staatliche Stellen Telekommunikationsunternehmen zur Erhebung, Speicherung oder Herausgabe von Verbindungsdaten verpflichten, greifen in das Fernmeldegeheimnis ein. Zudem erstreckt sich die Schutzwirkung des Grundrechts auf den Prozess der Informations- und Datenverarbeitung, der sich daran anschließt, sowie auf die Verwendung gewonnener Informationen. Daher ist jedes Erfassen, Speichern, Abgleichen, Auswerten, Selektieren und Übermitteln von Telekommunikationsdaten ein weiterer Eingriff.[34]

Beschränkungen des Fernmeldegeheimnisses dürfen gemäß Art. 10 Abs. 2 S. 1 GG nur aufgrund eines Gesetztes angeordnet werden. Ein solches Gesetz muss, damit es verfassungsgemäß ist, bestimmte Anforderungen erfüllen. Unter anderem ist der Grundsatz der Normenbestimmtheit und Normenklarheit zu wahren. Dies bedeutet, dass Anlass, Zweck und Grenzen des Eingriffs im Gesetz bereichsspezifisch, präzise und klar festgelegt werden müssen.[35] Außerdem muss mit dem Gesetz ein legitimer Zweck (etwa die rechtzeitige Erkennung bestimmter Gefahrenlagen) verfolgt werden, das Gesetz muss zur Erreichung dieses Zwecks geeignet und erforderlich sein, und es muss im engeren Sinne verhältnismäßig sein, d.h. die Beschränkung muss in einem angemessenen Verhältnis zu Gewicht und Bedeutung des Grundrechts stehen.[36] Unverhältnismäßig und daher verfassungswidrig wäre beispielsweise eine gesetzliche Regelung, die auf eine

32 Zum Schutzbereich des Fernmeldegeheimnisses siehe BVerfGE 67, 157 (172); 85, 386 (396); 100, 313 (358); 106, 28 (36); 110, 33 (53); 115, 166 (183); 120, 274 (307); 130, 151 (179). Siehe auch Thomas Schwabenbauer, »Kommunikationsschutz durch Art. 10 GG im digitalen Zeitalter«, in: *Archiv des öffentlichen Rechts*, 137 (2012), S. 1–41.

33 BVerfGE 115, 166 (183ff); 124, 43 (55); differenzierend Schwabenbauer, »Kommunikationsschutz« [wie Fn. 32], S. 9ff.

34 BVerfGE 100, 313 (359, 366f); 107, 299 (313); 125, 260 (309f).

35 BVerfGE 110, 33 (53).

36 Zum Grundsatz der Verhältnismäßigkeit generell Hans D. Jarass, »Art. 20 GG«, in: Hans D. Jarass/Bodo Pieroth (Hg.), *Grundgesetz für die Bundesrepublik Deutschland. Kommentar*, 10. Aufl., München 2009, S. 474–527 (509ff).

möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten abzielen würde. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört laut Bundesverfassungsgericht zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland.[37]

Außerdem hat das Bundesverfassungsgericht entschieden, dass heimliche Überwachungsmaßnahmen staatlicher Stellen stets einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren haben, dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt.[38] Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diesen Kernbereich nicht rechtfertigen. Insoweit findet auch keine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes statt. Für die Beantwortung der Frage, ob ein Sachverhalt im Einzelfall dem Kernbereich privater Lebensgestaltung zuzuordnen ist, kommt es unter anderem darauf an, ob der Sachverhalt höchstpersönlichen Charakter hat und ob der Betroffene diesen Sachverhalt überhaupt geheim halten will. Geschützt sind insbesondere innere Vorgänge wie Empfindungen und Gefühle, Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art sowie Ausdrucksformen der Sexualität. Nicht zum Kernbereich privater Lebensgestaltung gehören hingegen Äußerungen, die in einem unmittelbaren Bezug zu konkreten strafbaren Handlungen stehen, wie etwa Angaben über geplante oder begangene Straftaten.[39]

Da bei der Anordnung oder Durchführung einer Telekommunikationsüberwachung nicht sicher vorhersehbar ist, welchen Inhalt die Gespräche haben werden, ist nicht auszuschließen, dass durch eine Abhörmaßnahme auch Kommunikation erfasst wird, die den Kernbereich privater Lebensgestaltung betrifft. Diesem Problem trägt das Bundesverfassungsgericht durch ein zweistufiges Schutzkonzept Rechnung. In erster Linie ist darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten soweit wie möglich unterbleibt. Werden solche Daten ausnahmsweise erhoben, weil eine besondere Gefährdungslage gegeben ist und sich die Kernbereichsrelevanz vorher nicht klären lässt, so dürfen die betreffenden Daten jedenfalls nicht gespeichert, verwertet oder weitergegeben werden, sondern sie sind unverzüglich zu löschen.[40] Auch im Übrigen kommt dem Erfordernis verfahrensmäßiger Schutzvorkehrungen bei Eingriffen in Art. 10 GG besondere Bedeutung zu. Darunter fallen etwa die Pflicht zur Kennzeichnung erhobener Daten, bestimmte Mitteilungspflichten gegenüber dem Betroffenen und die Pflicht zur Vernichtung von Daten, sobald sie für die festgelegten Zwecke oder den gerichtlichen Rechtsschutz nicht mehr erforderlich sind.[41]

Das Grundrecht auf informationelle Selbstbestimmung und das Konzept personenbezogener Daten

Das Grundrecht auf informationelle Selbstbestimmung stellt eine Ausprägung des allgemeinen Persönlichkeitsrechts dar, das durch Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG geschützt ist. Es dient dem Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten und gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[42]

Das Recht auf informationelle Selbstbestimmung hat allerdings Auffangcharakter. Dies bedeutet, dass es ausschließlich dann zur Anwendung kommt, wenn durch die jeweilige Maßnahme nicht speziellere Rechte wie das Fernmeldegeheiminis (Art. 10 GG) oder die Unverletzlichkeit der Wohnung (Art. 13 GG) in ihrem Schutzbereich berührt sind.[43]

Der Schutzumfang des Grundrechts

Der Schutzumfang des Grundrechts auf informationelle Selbstbestimmung beschränkt sich nicht auf Informationen, die bereits ihrer Art nach sensibel sind. Auch der Umgang mit personenbezogenen Daten, die für sich genommen nur geringen Informationsgehalt haben, kann je nach Verarbeitung und Verknüpfung erhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit der Betroffenen haben. So hat das Bundesverfassungsgericht festgestellt, dass es unter den Bedingungen der elektronischen Daten-

37 BVerfGE 125, 260 (323f).
38 Siehe unter anderem BVerfGE 34, 238 (245f); 80, 367 (373ff); 109, 279 (313ff); 113, 348 (390ff); 120, 274 (335 ff); 129, 208 (245ff).
39 BVerfGE 80, 367 (375); 109, 279 (319); 113, 348 (391).
40 BVerfGE 113, 348 (392); 120, 274 (337ff).
41 BVerfGE 100, 313 (359ff).
42 BVerfGE 65, 1 (43).
43 Vgl. z.B. BVerfGE 100, 313 (358).

verarbeitung keine schlechthin belanglosen personenbezogenen Daten mehr gibt.[44] Zum Beispiel stellt die Zuordnung von Telekommunikationsnummern zu bestimmten Anschlussinhabern einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.[45]

Eingriffe in das Grundrecht auf informationelle Selbstbestimmung bedürfen ebenfalls einer speziellen gesetzlichen Grundlage.[46] Ein solches Gesetz muss den Verwendungszweck der erhobenen Daten bereichsspezifisch und präzise bestimmen, Schutzvorkehrungen gegen eine Zweckentfremdung bei der Datenverarbeitung treffen und Aufklärungs-, Auskunfts- und Löschungspflichten vorsehen.[47] Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche Stellen des Bundes gilt grundsätzlich das Bundesdatenschutzgesetz (BDSG).[48] Darüber hinaus existieren zahlreiche datenschutzrechtliche Spezialregelungen, unter anderem im BND-Gesetz (BNDG) und im Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz, G 10).

Anknüpfungspunkt: Daten mit Personenbezug

Das informationelle Selbstbestimmungsrecht und das Datenschutzrecht sind nur einschlägig, soweit es sich um personenbezogene Daten natürlicher Personen handelt. Daten, die juristische Personen betreffen und keinen personalen Bezug aufweisen, fallen nicht in den sachlichen Anwendungsbereich der Datenschutzgesetze. Die Vertraulichkeit solcher Informationen wird, je nachdem ob es sich um juristische Personen des öffentlichen Rechts oder des Privatrechts handelt, durch andere Vorschriften garantiert. Geschäfts- und Betriebsgeheimnisse sind beispielsweise durch Art. 12 und 14 GG geschützt.

§ 3 Abs. 1 BDSG definiert personenbezogene Daten als »Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)«. Von zentraler Bedeutung ist, wann eine Person als bestimmbar anzusehen ist. Die Beantwortung dieser Frage wirft gerade im Kontext digitaler Kommunikation erhebliche Probleme auf. So bedarf es der Klärung, anhand welcher Kommunikationsmetadaten unter welchen Voraussetzungen eine Person tatsächlich bestimmt werden kann. Stellt beispielsweise die IP-Adresse eines Internetnutzers, die ein Websitebetreiber bei einem Zugriff auf seine Website speichert, ein personenbezogenes Datum dar, wenn nur ein Dritter, etwa der Zugangsanbieter, über das zur Identifizierung des Nutzers erforderliche Zusatzwissen verfügt?[49] Nach herrschender Auffassung ist ein Personenbezug zu verneinen, sofern die Bestimmung des Betroffenen für die verantwortliche Stelle mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft verbunden ist. Außerdem müsse die jeweilige Stelle rechtlich befugt sein, die zur Bestimmung des Betroffenen notwendigen Maßnahmen zu veranlassen (relativer Maßstab).[50] Dem wird zum Teil entgegengehalten, dass es nicht auf die individuellen Verhältnisse der verantwortlichen Stelle ankomme, sondern dass ein Personenbezug auch dann gegeben sein könne, wenn ausschließlich ein Dritter in der Lage sei, die Identität des Betroffenen festzustellen (objektiver Maßstab).[51]

Auf europarechtlicher Ebene sind diese Fragen bislang ebenso wenig geklärt. Nach der Europäischen Datenschutzrichtlinie von 1995 gilt eine Person als bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann, »insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind«.[52] Dabei sollen alle Mittel zu berücksichtigen sein, »die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu be-

44 BVerfGE 120, 378 (398f).

45 Demgegenüber liegt in der Zuordnung von dynamischen IP-Adressen ein Eingriff in Art. 10 Abs. 1 GG (BVerfGE 130, 151).

46 Zur Schrankentrias des Art. 2 Abs. 1 GG siehe Bodo Pieroth/Bernhard Schlink/Thorsten Kingreen/Ralf Poscher, *Grundrechte Staatsrecht II*, 31. Aufl., Heidelberg 2015, S. 102ff.

47 BVerfGE 65, 1 (46).

48 Zur Definition des Erhebens, Verarbeitens und Nutzens siehe § 3 Abs. 3 bis 5 BDSG. Danach stellt das Übermitteln personenbezogener Daten einen Unterfall der Verarbeitung dar.

49 Diese Frage hat der Bundesgerichtshof (BGH) im Oktober 2014 dem Gerichtshof der Europäischen Union zur Vorabentscheidung vorgelegt (Beschluss VI ZR 135/13 vom 28.10.2014).

50 Siehe BGH, Beschluss vom 28.10.2014 [wie Fn. 49], Rn. 25f mwN und Rn. 31f. Danach können dieselben Daten für eine Stelle personenbezogen und für eine andere Stelle nicht personenbezogen sein.

51 Siehe die Nachweise in BGH, Beschluss vom 28.10.2014 [wie Fn. 49], Rn. 24.

52 Art. 2 lit. a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

stimmen«.[53] Im Entwurf für eine neue EU-Datenschutzverordnung, die 2018 in Kraft treten soll, wurde der entsprechende Passus in der Definition personenbezogener Daten geringfügig modifiziert und den Gegebenheiten digitaler Erfassungsmöglichkeiten angepasst.[54] Aus den Erwägungsgründen des Entwurfs geht nun aber hervor, dass die Einschaltung eines Dritten zur Identifizierung des Betroffenen per se ein vernünftigerweise einzusetzendes Mittel sein kann. Bei der Prüfung, ob der Mitteleinsatz im konkreten Fall vernünftig wäre, sollten alle objektiven Faktoren Berücksichtigung finden, etwa der Kosten- und Zeitaufwand sowie die verfügbare Technologie.[55] Abzuwarten bleibt, wie sich der Gerichtshof der Europäischen Union zu dieser Thematik äußern wird.[56]

Für die Reichweite der Befugnisse und datenschutzrechtlichen Bindungen der Nachrichtendienste besitzt die Frage, wann Kommunikationsmetadaten einen Personenbezug aufweisen, jedenfalls erhebliche Relevanz. Vor allem geht es um die Frage, welcher Aufwand zur Identifizierung einer Person anhand von Metadaten als verhältnismäßig anzusehen ist.[57]

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Eine weitere lückenschließende Rechtsfortbildung hat das Bundesverfassungsgericht 2008 betrieben, indem es das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (»IT-Grundrecht«) aus dem allgemeinen Persönlichkeitsrecht ableitete.[58] Dies war nach Ansicht des Gerichts erforderlich, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen könne. Anwendbar ist dieses Grundrecht nur, soweit weder speziellere Grundrechte wie Art. 10 oder Art. 13 GG noch das Recht auf informationelle Selbstbestimmung hinreichenden Schutz bieten. Anders als das Fernmeldegeheimnis nach Art. 10 GG erfasst das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht den laufenden Kommunikationsvorgang und seine Inhalte und Umstände. Vielmehr geht es darum, die Systeme vor technischer Infiltration und heimlicher Ausspähung zu schützen. Durch derartige Maßnahmen wird das allgemeine Persönlichkeitsrecht unter Umständen weitaus stärker

53 Ziffer 26 der Erwägungsgründe der Richtlinie 95/46/EG [wie Fn. 52].

54 Council of the European Union, »Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)«, 2012/0011 (COD), 15.12.2015, Art. 4 (1): »›personal data‹ means any information relating to an identified or identifiable natural person (›data subject‹); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person«.

55 Ziffer 23 der Erwägungsgründe des Entwurfs [wie Fn. 54]: »[...] Data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.«

56 Siehe Fn. 49.

57 Der BND scheint davon auszugehen, dass es sich zum Beispiel bei ausländischen Telefonnummern prinzipiell nicht um personenbezogene Metadaten handelt, da insoweit – anders als bei deutschen Telefonnummern – keine rechtliche Handhabe dafür bestehe, den Anschlussinhaber durch eine Abfrage beim ausländischen Telekommunikationsanbieter ohne weiteres zu ermitteln. Siehe dazu die Vernehmung der Zeugin Dr. H. F. und des Zeugen A. F. vor dem NSA-Untersuchungsausschuss, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, Stenografisches Protokoll der 16. Sitzung (vorläufige Fassung), 9.10.2014, S. 25ff; Stenografisches Protokoll der 41. Sitzung (vorläufige Fassung), 19.3.2015, S. 118f. Ein Großteil der Zeugenvernehmung findet in öffentlichen Sitzungen statt. Aktuelle Informationen über einzelne Sitzungen veröffentlicht der Ausschuss auf seiner Website [wie Fn. 2]. Außerdem wird über seine Sitzungen regelmäßig in Blogs und Podcasts berichtet. Siehe vor allem <https://netzpolitik.org>. Zur Berichterstattung durch die Presse siehe unter anderem <www.zeit.de/thema/nsa-affaere> und <www.spiegel.de/thema/bnd/>. Einzelne stenographische Protokolle finden sich auf der Enthüllungsplattform WikiLeaks, <https://wikileaks.org/bnd-nsa/sitzungen/>. Zur Problematik der Metadaten siehe auch Graulich, *Nachrichtendienstliche Fernmeldeaufklärung* [wie Fn. 1], S. 87f. Kritisch dazu Andre Meister, »Lieber Bundesnachrichtendienst: Wir erklären, warum Metadaten sehr wohl personenbezogene Daten sind«, 14.11.2014, <https://netzpolitik.org/2014/lieber-bundesnachrichtendienst-wir-erklaeren-warum-metadaten-sehr-wohl-personenbezogene-daten-sind/> (Zugriff jeweils am 12.4.2016).

58 BVerfGE 120, 274 (302ff).

gefährdet als durch die Überwachung laufender Kommunikation. Die Abgrenzung zum Recht auf informationelle Selbstbestimmung ergibt sich daraus, dass ein Zugriff auf persönliche Daten, die der Einzelne informationstechnischen Systemen anvertraut und bei deren Nutzung zwangsläufig generiert, in seinem Gewicht über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinausgeht.

Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit ist dann einschlägig, wenn der Staat Systeme ausspäht, die personenbezogene Daten in so großem Umfang und in solcher Vielfalt enthalten können, dass durch den Zugriff ein Einblick in wesentliche Teile der Lebensgestaltung einer Person oder gar ein aussagekräftiges Bild ihrer Persönlichkeit gewonnen werden kann. Dies betrifft Zugriffe auf stationäre Computer ebenso wie auf Smartphones oder vergleichbare Systeme, in denen Daten gespeichert sind, deren Auswertung weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen.[59] Ungeklärt ist bislang noch, wo die Grenze zwischen dem geschützten System und der das System umgebenden, nicht vom Schutzbereich des Grundrechts erfassten Infrastruktur verläuft.

Wie das Recht auf informationelle Selbstbestimmung unterliegt auch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewissen Einschränkungen. Eingriffe bedürfen einer verfassungsmäßigen gesetzlichen Grundlage. Insoweit gelten vergleichbare Anforderungen wie für Gesetze, die zu Eingriffen in das Fernmeldegeheimnis nach Art. 10 GG ermächtigen.[60] Die heimliche längerfristige Infiltration informationstechnischer Systeme zur Gewinnung von Daten stellt jedoch einen besonders schwerwiegenden Grundrechtseingriff dar. Daher sind solche Maßnahmen im Rahmen einer präventiven Zielsetzung nur dann zulässig, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Als überragend wichtige Rechtsgüter hat das Bundesverfassungsgericht neben Leib, Leben und Freiheit von Personen auch solche Güter der Allgemeinheit eingestuft, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen gefährdet. Darüber hinaus ist für einen solchen Zugriff eine richterliche Anordnung erforderlich.[61]

Grundrechtsberechtigte

Das Fernmeldegeheimnis, das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sind Grundrechte, auf die sich jede natürliche Person berufen kann (im Gegensatz zu den Grundrechten, die speziell als Deutschengrundrechte ausgestaltet sind).[62] Auf die Staatsangehörigkeit des Betroffenen kommt es somit nicht an.

Auch deutsche Amtsträger genießen prinzipiell Grundrechtsschutz, sofern sie im Rahmen ihrer amtlichen Tätigkeit als Grundrechtsträger betroffen sind. Sie müssen aber unter Umständen Einschränkungen hinnehmen, die sich aus ihrer amtlichen Funktion ergeben.[63] Dazu hat sich das Bundesverwaltungsgericht geäußert, und zwar mit Blick auf das Recht auf informationelle Selbstbestimmung, das Recht auf Privatsphäre und das Recht am gesprochenen Wort. Der aus diesen Rechten erwachsende Schutz erfasse private wie amtsbezogene Gespräche und Informationen und erstrecke sich sogar auf Telefonate in dienstlichen Büro- und Sitzungsräumen. So benötigten und verdienten auch gewählte Amtsträger grundrechtlichen Schutz davor, im Amt von anderen Stellen heimlich überwacht und abgehört zu werden.[64] Darüber hinaus steht solchen Personen selbstverständlich ein geschützter privater Rückzugsbereich zu.[65]

Inländische juristische Personen kommen gemäß Art. 19 Abs. 3 GG als Grundrechtsträger in Betracht, soweit die Grundrechte »ihrem Wesen nach auf diese anwendbar sind«, d.h. soweit das betreffende Grundrecht auch korporativ ausgeübt werden kann. Juristische Personen und Personenvereinigungen des Privat-

59 BVerfGE 120, 274 (305ff, 313f).

60 Christian Bumke/Andreas Voßkuhle, Casebook Verfassungsrecht, 7. Aufl., Tübingen 2015, S. 110f.

61 BVerfGE 120, 274 (326ff).

62 Hans D. Jarass, »Art. 10 GG«, in: Jarass/Pieroth, *Grundgesetz* [wie Fn. 36], S. 296–305 (300); ders., »Art. 2 GG«, ebd., S. 58–100 (76).

63 Pieroth/Schlink/Kingreen/Poscher, *Grundrechte* [wie Fn. 46], S. 48. Zur Frage der Einschränkung siehe unter anderem das Minderheitenvotum zur Kopftuchentscheidung des Bundesverfassungsgerichts, BVerfGE 108, 282 (314ff).

64 BVerwGE 121, 115 (125f). Siehe auch BVerwGE 116, 104 (112).

65 BVerfGE 101, 361 (383).

rechts, wie zum Beispiel Unternehmen oder private Stiftungen, können sich daher ebenfalls auf Art. 10 GG sowie auf das Recht auf informationelle Selbstbestimmung und auf das IT-Grundrecht berufen.[66] Der Schutz von Betriebs- und Geschäftsgeheimnissen ergibt sich aus Art. 12 und 14 GG. Juristischen Personen des öffentlichen Rechts bieten die Grundrechte – von wenigen Ausnahmen abgesehen – keinen Schutz.[67]

Definitiv nicht zum Kreis der Grundrechtsberechtigten zählen ausländische juristische Personen und Personenvereinigungen.[68] Daher stellt zum Beispiel die Überwachung der Kommunikation ausländischer Regierungseinrichtungen keinen Eingriff in Art. 10 GG dar.[69] Ob ein Unternehmen oder eine Nichtregierungsorganisation als ausländisch anzusehen ist, richtet sich nach herrschender Meinung danach, wo sich der Sitz, d.h. der tatsächliche Ort des Verwaltungszentrums, befindet. Auskunft gibt etwa die Eintragung in ein inländisches oder ausländisches Register. Auf die Staatsangehörigkeit der dahinter stehenden natürlichen Personen kommt es hingegen nicht an.[70] Allerdings wird vertreten, dass der Grundrechtsschutz, der inländischen juristischen Personen zustehe, auch juristischen Personen zuteilwerden müsse, die ihren Sitz in einem anderen Mitgliedstaat der Europäischen Union haben (Gleichstellung durch Anwendungserweiterung des Art. 19 Abs. 3 GG).[71]

Der BND scheint davon auszugehen, dass Kommunikation, die über ein Endgerät läuft, das anhand seiner Kennung einer ausländischen juristischen Person (etwa einem ausländischen Unternehmen oder einer Nichtregierungsorganisation) zugeordnet wird, prinzipiell ohne grundrechtlich gebotene Einschränkung überwacht werden darf.[72] Der Gedanke, dass natürliche Personen schlechthin keinen Grundrechtsschutz genießen, während sie als Funktionsträger für ausländische juristische Personen tätig sind, lässt sich mit den Prinzipien einer effektiven Grundrechtswahrung kaum vereinbaren.[73] Besonders schwierig ist es jedoch, trennscharf zwischen der Rechtssphäre der (geschützten) natürlichen Person und der Rechtssphäre der (ungeschützten) ausländischen juristischen Person zu unterscheiden, wenn die natürliche Person für die juristische Person am Telefon oder per E-Mail kommuniziert. In diesem Vorgang können beide Rechtssphären miteinander verschmelzen. Konkret stellt sich die Frage, ob ein solches Telefonat oder eine solche E-Mail dem Schutz des Fernmeldegeheimnisses nach Art. 10 GG unterliegt. Allenfalls ließe sich eine Differenzierung danach vornehmen, welche Inhalte der natürlichen und welche der juristischen Person zuzuordnen sind. Dies würde aber im Fall der nachrichtendienstlichen Überwachung voraussetzen, dass das Gespräch überhaupt in vollem Umfang abgehört und dann ausgewertet werden darf. Sofern man dies für zulässig erachtet und das Schutzinteresse der natürlichen Person im Einzelfall tatsächlich dem Interesse an der Überwachung der juristischen Person unterordnet, müssen aber verfahrensmäßige Schutzvorkehrungen (siehe dazu die Ausführungen auf S. 14) getroffen werden, um den durch Art. 10 GG garantierten Schutz der privaten Inhalte zu gewährleisten.

Die Reichweite der Grundrechtsbindung

Gemäß Art. 1 Abs. 3 GG binden die Grundrechte die Gesetzgebung, die vollziehende Gewalt und die Rechtsprechung als unmittelbar geltendes Recht. Der räumliche Schutzbereich der Grundrechte wirft jedoch Fragen auf. Umstritten ist insbesondere, ob der BND auch dann an die Grundrechte gebunden ist,

66 Zu Art. 10 GG siehe BVerfGE 100, 313 (356); differenzierend zum Recht auf informationelle Selbstbestimmung, das sich für juristische Personen allein aus Art. 2 Abs. 1 und nicht aus Art. 1 Abs. 1 GG ergibt, siehe BVerfGE 106, 28 (42ff); 118, 168 (203f).

67 Ausnahmen gelten für Kirchen, Universitäten und öffentlich-rechtliche Rundfunkanstalten sowie für andere juristische Personen des öffentlichen Rechts, bei denen nicht eine gesetzlich zugewiesene und geregelte öffentliche Aufgabe, sondern die Interessenwahrnehmung der Mitglieder im Vordergrund steht. Dazu Bumke/Voßkuhle, *Casebook Verfassungsrecht* [wie Fn. 60], S. 9ff.

68 BVerfGE 100, 313 (363f). Zu den Besonderheiten siehe Hans D. Jarass, »Art. 19 GG«, in: Jarass/Pieroth, *Grundgesetz* [wie Fn. 36], S. 446–473 (456).

69 Hans-Jürgen Papier, »Das ist vom Grundgesetz nicht gedeckt«, Interview, in: *Süddeutsche Zeitung*, 4.9.2014, S. 6.

70 BVerfGE 21, 207 (209); Bumke/Voßkuhle, *Casebook Verfassungsrecht* [wie Fn. 60], S. 8; Jarass, »Art. 19 GG« [wie Fn. 68], S. 456.

71 BVerfGE 129, 78 (94ff).

72 Zur Einbettung des »Funktionsträger«-Ansatzes in die Argumentation des BND siehe unter anderem die Vernehmung des Zeugen A. F. [wie Fn. 57], S. 132ff, 160f, und des Zeugen Dr. Stefan Burbaum, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, Stenografisches Protokoll der 24. Sitzung (vorläufige Fassung), 27.11.2014, S. 45ff, 64. Siehe dazu auch die Ausführungen in dieser Studie auf S. 30.

73 Zur Grundrechtsberechtigung natürlicher Personen, die sich zu Personenmehrheiten und Organisationen zusammenschließen, siehe Pieroth/Schlink/Kingreen/Poscher, *Grundrechte* [wie Fn. 46], S. 44.

wenn er im Ausland aktiv wird und dadurch Ausländer betroffen sind.

In seinem Urteil von 1999 zur Telekommunikationsüberwachung hat sich das Bundesverfassungsgericht unter anderem mit der Frage auseinandergesetzt, wie weit der Schutz durch das Fernmeldegeheimnis nach Art. 10 GG in räumlicher Hinsicht reicht.[74] In dem Verfahren vertrat die Bundesregierung die Auffassung, dass Art. 10 GG zwar Deutsche und Ausländer schütze; der Sachverhalt, der als Grundrechtseingriff zu qualifizieren sei, müsse aber einen Bezug zum Territorium der Bundesrepublik aufweisen. Die Auffassung, wonach die deutsche Staatsgewalt überall und unterschiedslos an die Grundrechte gebunden sei, könne keine allgemeine Anerkennung beanspruchen. Die deutsche Staatsgewalt sei im Ausland nur dann an die Grundrechte gebunden, wenn sie dort kraft Völkerrechts oder mit besonderer Zulassung durch den jeweiligen Territorialstaat wirksam werde und der Eingriff auf der Gebietshoheit oder der Personalhoheit Deutschlands beruhe. Eine strategische Aufklärung des Fernmeldeverkehrs von Ausländern im Ausland durch den BND falle daher nicht unter Art. 10 GG.[75]

Dazu hat das Bundesverfassungsgericht zunächst ausgeführt, dass sich aus Art. 1 Abs. 3 GG, wonach die drei Gewalten unmittelbar an die Grundrechte gebunden sind, noch keine abschließende Festlegung der räumlichen Geltung der Grundrechte ergebe. Die Reichweite der Grundrechte sei (unter Beachtung eventueller Grenzen, die sich aus den allgemeinen Regeln des Völkerrechts nach Art. 25 GG ergeben) aus dem Grundgesetz selbst zu ermitteln. Je nachdem, welche Verfassungsnorm einschlägig sei, könnten Differenzierungen zulässig und geboten sein. Im Hinblick auf Art. 10 GG gelte Folgendes: Bereits durch die Erfassung und Aufzeichnung des Telekommunikationsverkehrs mit Hilfe der auf deutschem Boden stationierten Empfangsanlagen des BND werde eine technisch-informationelle Beziehung zu den jeweiligen Kommunikationsteilnehmern und ein – den Eigenarten von Daten und Informationen entsprechender – Gebietskontakt hergestellt. Außerdem finde auch die Auswertung der so erfassten Telekommunikationsvorgänge durch den BND auf deutschem Boden statt. Unter diesen Umständen sei eine Kommunikation im Ausland mit staatlichem Handeln im Inland derart verknüpft, dass eine Bindung an Art. 10 GG selbst dann bestehe, wenn man dafür einen hinreichenden territorialen Bezug voraussetzen wollte.[76] Ob ein solcher territorialer Bezug überhaupt bestehen müsse, ließ das Gericht offen.

Hinzu kommt nach Ansicht von Kommentatoren, dass der BND als im Inland ansässige Behörde handle. Stelle man auf diese territorialen Bezüge zum Bundesgebiet ab, sei es unerheblich, ob sich die Überwachung auf Telekommunikationsbeziehungen zwischen Deutschland und dem Ausland konzentriere oder ob die Maßnahmen dazu dienten, Ausland-zu-Ausland-Verkehre abzufangen. In beiden Fällen bedürfe es einer verfassungsmäßigen gesetzlichen Grundlage, die den spezifischen Anforderungen von Art. 10 GG genügen müsse.[77]

Das Bundesverfassungsgericht hat allerdings keine Aussage darüber getroffen, wie der Fall zu beurteilen wäre, wenn zur Erfassung von Telekommunikationsbeziehungen Anlagen außerhalb des Territoriums der Bundesrepublik genutzt würden und wenn gegebenenfalls sogar die Verarbeitung und Nutzung der Daten durch den BND im Ausland erfolgen würde. Bereits früher hatte das Bundesverfassungsgericht entschieden, dass die Grundrechte die deutsche öffentliche Gewalt auch binden, soweit Wirkungen ihrer Betätigung außerhalb des Hoheitsbereichs der Bundesrepublik eintreten.[78] In der Literatur wird dementsprechend überwiegend davon ausgegangen, dass Organe des Staates auch dann an Grundrechte gebunden sind, wenn sie als solche im Ausland handeln.[79] Unter der Annahme, dass der räumliche Anwendungsbereich der Grundrechte den gesamten Wirkungsbereich deutscher Staatsgewalt erfasst, ist es unerheblich, wo sich die Empfangsanlagen und andere Einrichtungen befinden, über die der BND Daten erfasst, wo der Zugriff auf ein Kabel erfolgt, wo sich die Kommunikationsteilnehmer aufhalten oder wo die Ver-

74 BVerfGE 100, 313.

75 Die Auffassung der Bundesregierung ist im Urteil (BVerfGE 100, 313) auf S. 338f zusammengefasst.

76 BVerfGE 100, 313 (362ff).

77 Berthold Huber, »Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10)«, in: Wolf-Rüdiger Schenke/Kurt Graulich/Josef Ruthig (Hg.), *Sicherheitsrecht des Bundes*, München 2014, S. 1349–1462 (1355).

78 BVerfGE 6, 290 (295); 57, 9 (23).

79 Siehe unter anderem Christian Hillgruber, »Art. 1 GG«, in: Volker Epping/Christian Hillgruber (Hg.), *Beck'scher Online-Kommentar GG*, 26. Aufl., München 2015, Rn. 76; Hans D. Jarass, »Art. 1 GG«, in: Jarass/Pieroth, *Grundgesetz* [wie Fn. 36], S. 37–57 (52) mwN; Pieroth/Schlink/Kingreen/Poscher, *Grundrechte* [wie Fn. 46], S. 55.

arbeitung und Nutzung der Daten durch den BND stattfindet.[80]

Die Unterscheidung zwischen In- und Ausland – zumindest was die Übertragungswege elektronischer Kommunikation angeht – verliert wegen der technologischen Entwicklung ohnehin an Bedeutung. Oben wurde bereits darauf hingewiesen, dass ein Telefonat oder E-Mail-Verkehr zwischen zwei Kommunikationsteilnehmern in Deutschland durchaus über erhebliche Umwege im Ausland abgewickelt werden kann, ohne dass dies für die Teilnehmer vorhersehbar wäre. Auf solche Umstände kann es beim Schutz des Fernmeldegeheimnisses nicht ankommen. Entscheidend ist vielmehr, dass Grundrechtsträger, die sich bestimmter Kommunikationsmittel bedienen, darauf vertrauen dürfen, dass ihre Kommunikation nach Maßgabe des Art. 10 GG vor dem Zugriff deutscher Behörden auf dem gesamten Übertragungsweg geschützt ist.[81]

Offen ließ das Bundesverfassungsgericht in seinem Urteil von 1999 schließlich, ob ausländische Kommunikationsteilnehmer im Ausland ebenfalls durch Art. 10 GG geschützt sind. Dies wäre zum Beispiel der Fall, wenn der BND Telekommunikationsverkehre zwischen afghanischen Staatsangehörigen in Afghanistan überwacht. Auch dazu findet sich in der Literatur eine eindeutige Haltung: Jene Grundrechte, die wie das Fernmeldegeheimnis oder das allgemeine Persönlichkeitsrecht nicht speziell als Deutschenrechte ausgestaltet seien, böten in ihrer abwehrrechtlichen Dimension auch Ausländern Schutz, die im Ausland der deutschen öffentlichen Gewalt begegneten.[82] So sei die deutsche Staatsgewalt bei extraterritorialem Handeln an Art. 10 GG gebunden, ohne dass die Frage der Staatsangehörigkeit des Betroffenen eine Rolle spiele.[83] Im Zusammenhang mit den gesetzlichen Befugnissen des BND wird auf diese Fragen noch einmal zurückzukommen sein.

80 Siehe dazu auch Wolfgang Hoffmann-Riem, *Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014*, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, MAT A SV-2/1, zu A-Drs. 54, 16.5.2014, S. 11f; siehe auch Matthias Bäcker, *Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014. Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes*, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, MAT A SV-2/3, zu A-Drs. 54, 16.5.2014, S. 19f.

81 Hoffmann-Riem, *Stellungnahme zur Anhörung* [wie Fn. 80], S. 10.

82 Jarass, »Art. 1 GG« [wie Fn. 79], S. 52; Pieroth/Schlink/Kingreen/Poscher, *Grundrechte* [wie Fn. 46], S. 37.

83 Manfred Baldus, »Art. 10 GG«, in: Epping/Hillgruber, *Beck'scher Online-Kommentar GG* [wie Fn. 79], Rn. 21; siehe auch Bäcker, *Stellungnahme zur Anhörung* [wie Fn. 80], S. 19; Hans-Jürgen Papier, *Gutachterliche Stellungnahme*, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, MAT A SV-2/2, zu A-Drs. 54, 16.5.2014, S. 7.

Aktionen ausländischer Nachrichtendienste im Lichte der Grundrechte

Ein wichtiger Aspekt, der auch bei der Aufklärung der NSA-Affäre eine Rolle spielt, ist die mögliche Verantwortlichkeit deutscher Behörden für das Handeln ausländischer Geheimdienste in Deutschland. Die Grundrechtsbindung nach Art. 1 Abs. 3 GG betrifft zwar nur die durch das Grundgesetz konstituierte deutsche öffentliche Gewalt, nicht Organe anderer Staaten. Im Zusammenhang mit ausländischem hoheitlichem Handeln lässt sich aber unter Umständen eine grundrechtsrelevante Verantwortlichkeit deutscher Organe herleiten.

Zurechnung ausländischen hoheitlichen Handelns

Das Handeln ausländischer Organe lässt sich der Bundesrepublik zurechnen, wenn deutsche Stellen an hoheitlichen Handlungen solcher Organe mitwirken oder diese vollziehen.[84] Außerdem wird im wissenschaftlichen Diskurs argumentiert, dass auch Eingriffe zurechenbar sind, die mit Billigung oder Duldung deutscher Behörden erfolgen.[85] Eine Zurechnung scheidet hingegen aus, wenn die Bundesrepublik aus rechtlichen oder tatsächlichen Gründen daran gehindert ist, auf den Geschehensablauf, der zum Grundrechtseingriff führt, Einfluss zu nehmen. Die verfassungsrechtliche Verantwortlichkeit der deutschen Hoheitsgewalt und damit auch der Schutz der Grundrechte enden grundsätzlich dort, wo ein Vorgang in seinem wesentlichen Verlauf von einem anderen Staat unabhängig vom Willen der Bundesrepublik gestaltet wird.[86]

Soweit also Maßnahmen der NSA von deutschem Boden ausgehen und von deutschen Behörden gebilligt oder geduldet werden oder sogar auf einer Absprache beruhen, könnte prinzipiell eine Zurechnung der dadurch verursachten Grundrechtsbeeinträchtigungen in Betracht kommen. In welchem Umfang deutsche Behörden allerdings über die Aktivitäten der NSA in Deutschland informiert sind und inwieweit sie gegebenenfalls tatsächlich in der Lage sind, auf einzelne Vorgänge Einfluss zu nehmen, kann hier nicht beurteilt werden. Die umfangreichen Enthüllungen durch Edward Snowden dürften jedenfalls zu einer konkreteren Einschätzung dieser Aktivitäten beigetragen haben. Selbst wenn es im Einzelfall an den Voraussetzungen für eine Eingriffszurechnung fehlt, steht der deutsche Staat doch grundsätzlich in der Pflicht, sich schützend vor seine Grundrechtsträger zu stellen. Denn die Grundrechte sind nicht nur Abwehrrechte gegen den Staat; aus ihnen ergeben sich auch staatliche Schutzpflichten.

Grundrechtliche Schutzpflichten

Der Staat ist prinzipiell verpflichtet, den Einzelnen auch vor Grundrechtsbeeinträchtigungen zu schützen, die von Dritten ausgehen, etwa von anderen Staaten. Solche Schutzpflichten können sowohl auf die Verhinderung als auch auf die Beseitigung von Grundrechtsbeeinträchtigungen gerichtet sein. Sie betreffen in erster Linie den Gesetzgeber. Dem Schutzauftrag, der aus dem Grundrecht auf informationelle Selbstbestimmung erwächst, ist der Gesetzgeber beispielsweise durch den Erlass umfangreicher Regelungen zum Datenschutz nachgekommen. Da Art. 10 GG und das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ebenfalls Schutzpflichten begründen, hat der Staat etwa auch die Aufgabe, durch den Erlass geeigneter Regelungen und Standards dafür zu sorgen, dass die Informations- und Kommunikationsinfrastruktur funktionsfähig und sicher ist und dass die Grundrechtssphäre der Nutzer geschützt wird.[87] Sich im Rahmen der Europäischen Union und auf internationaler Ebene für entsprechende Normen und Standards einzusetzen ist Teil dieser Aufgabe.

84 Jarass, »Art. 1 GG« [wie Fn. 79], S. 52.

85 Papier, *Gutachterliche Stellungnahme* [wie Fn. 83], S. 7; siehe auch die mündliche Einlassung des Sachverständigen Bäcker im NSA-Untersuchungsausschuss, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, Stenographisches Protokoll der 5. Sitzung vom 22.5.2014, S. 18.

86 BVerfGE 66, 39 (62). Vgl. auch BVerfGE 55, 349 (362f); 57, 9 (23f).

87 Ausführlich dazu Hoffmann-Riem, *Stellungnahme zur Anhörung* [wie Fn. 80], S. 15ff.

Darüber hinaus kann es auch geboten sein, politischen und diplomatischen Druck auf Regierungen auszuüben, von denen Grundrechtsbeeinträchtigungen ausgehen.[88] Bei der Erfüllung seiner Schutzpflichten hat der Staat jedoch grundsätzlich einen weiten Einschätzungs-, Wertungs- und Gestaltungsspielraum, der im außenpolitischen Bereich besonders ausgeprägt ist.[89] Daher folgt aus einer grundrechtlichen Schutzpflicht in der Regel keine konkrete Handlungsvorgabe. Allerdings muss der Schutz angemessen und wirksam sein.[90]

Bezogen auf die nachrichtendienstliche Kooperation ergeben sich ebenfalls Schutzpflichten des Staates. Gestattet die Bundesrepublik ausländischen Diensten, im Rahmen einer Zusammenarbeit mit dem BND in Deutschland tätig zu sein, muss sichergestellt werden, dass die Zusammenarbeit grundrechtskonform abläuft. Dafür kann es erforderlich sein, dass entsprechende Kontroll-, Konsultations- und Reaktionsmechanismen geschaffen werden.[91] Ausländische Hoheitsakte dürfen von deutschen Stellen jedenfalls nicht um- oder durchgesetzt werden, wenn es dadurch zu einer Verletzung von Grundrechten käme.[92]

Fraglich ist aber, in welchem Umfang das aus den Grundrechten abgeleitete Schutzpflichtkonzept greifen kann, wenn die Grundrechtsbeeinträchtigung von einem anderen Staat ausgeht, auf dessen Verhalten der deutsche Staat tatsächlich keinen Einfluss nehmen kann, etwa weil es an der erforderlichen Kenntnis oder an der praktischen Durchsetzbarkeit eigener Rechtspositionen fehlt.[93] Politisch aussichtslos dürfte zudem die Idee sein, mit den USA ein völkerrechtlich verbindliches »No-Spy-Abkommen« zu schließen. Prinzipiell haben die USA kein Interesse daran, ihren Handlungsspielraum in diesem Bereich durch rechtliche Bindungen zu beschränken. Denkbar wären allenfalls partielle politische Zugeständnisse. Ob die Forderung nach solchen Konzessionen realistisch ist, hängt auch vom jeweiligen Stand der deutsch-amerikanischen Beziehungen und vom Arsenal der verfügbaren Druckmittel ab.

Im Übrigen kann es bei Bereichen, die in hohem Maße international reguliert sind, schwierig sein, den deutschen grundrechtlichen Schutzstandard vollständig durchzusetzen. Daher sieht es das Bundesverfassungsgericht als zulässig an, eine Minderung des Grundrechtsstandards bei internationalen Konstellationen in Kauf zu nehmen, wenn die Alternative darin bestünde, den Grundrechtsschutz völlig aufzugeben.[94]

Grundrechtliche Grenzen des Datenaustauschs mit ausländischen Nachrichtendiensten

Fraglich ist, welche Grenzen die Grundrechte einem Datenaustausch zwischen dem BND und ausländischen Nachrichtendiensten setzen. Eine Übermittlung von Daten durch den BND an ausländische Stellen darf nur dann erfolgen, wenn Vorkehrungen dafür getroffen werden, dass die weitere Verwendung der Daten nach rechtsstaatlichen Prinzipien erfolgt.[95] Welche gesetzlichen Regelungen dazu existieren, wird weiter unten noch ausführlicher beleuchtet (siehe S. 34).

Werden Informationen von einem ausländischen Nachrichtendienst in grundrechtsverletzender Weise (z.B. durch Folter) gewonnen und dem BND übermittelt, könnte dessen Grundrechtsbindung prinzipiell dagegen sprechen, dass er diese Informationen verwenden darf. Dies würde voraussetzen, dass der BND von den jeweiligen Umständen Kenntnis hat. Im Strafprozessrecht existieren strikte Beweisverwertungsverbote, soweit es sich um Fälle grundrechtswidriger Beweiserhebung handelt. Für den Bereich der Gefahrenabwehr gelten jedoch andere Prinzipien und Vorgaben als für die Strafverfolgung. Die Aufgabe des BND besteht darin, zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspoli-

88 Zu möglichen Maßnahmen siehe Carl-Wendelin Neubert, »Grundrechtliche Schutzpflicht des Staates gegen grundrechtsbeeinträchtigende Maßnahmen fremder Staaten am Beispiel der Überwachung durch ausländische Geheimdienste«, in: *Archiv des öffentlichen Rechts*, 140 (2015), S. 67–304 (278ff).

89 Kritisch dazu Neubert, »Grundrechtliche Schutzpflicht« [wie Fn. 88], S. 286ff.

90 BVerfGE 115, 118 (159); 88, 203 (254). Das Bundesverfassungsgericht kann die Verletzung einer Schutzpflicht nur feststellen, wenn Schutzvorkehrungen überhaupt nicht getroffen worden sind, wenn die getroffenen Maßnahmen offensichtlich ungeeignet oder völlig unzulänglich sind oder wenn sie erheblich hinter dem Schutzziel zurückbleiben, BVerfGE 92, 26 (46); 125, 39 (78f).

91 Christoph Gusy, »Gesetz über den Bundesnachrichtendienst (BND-Gesetz – BNDG)«, in: Schenke/Graulich/Ruthig (Hg.), *Sicherheitsrecht* [wie Fn. 77], S. 1261–1303 (1278).

92 Pieroth/Schlink/Kingreen/Poscher, *Grundrechte* [wie Fn. 46], S. 54.

93 Dazu Peter Schaar, »Globale Überwachung und digitale Souveränität«, in: *Zeitschrift für Außen- und Sicherheitspolitik*, 8 (2015), S. 447–459 (455).

94 BVerfGE 92, 26 (42).

95 Papier, *Gutachterliche Stellungnahme* [wie Fn. 83], S. 8f.

tischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen zu sammeln und auszuwerten (§ 1 Abs. 2 BND-Gesetz); und bei der strategischen Telekommunikationsüberwachung geht es darum, bestimmte Gefahrenlagen zu erkennen (§ 5 G 10). Selbst wenn der BND Daten an Strafverfolgungsbehörden übermittelt (§ 7 Abs. 4 S. 2 G 10), stellt diese Übermittlung noch keine Beweisverwertung im strafprozessualen Sinne dar. Ein eventuelles Beweisverwertungsverbot würde erst die Strafverfolgungsbehörden treffen. Aus gefahrenabwehrrechtlicher Sicht ist indes nicht nachvollziehbar, weshalb der BND durch die Grundrechte generell und ausnahmslos daran gehindert sein sollte, solche Informationen zur Kenntnis zu nehmen und daraus Schlüsse zu ziehen. Daher lässt sich durchaus argumentieren, dass der BND unter sorgfältiger Abwägung im Einzelfall – d.h. unter Berücksichtigung der Wertigkeit des gefährdeten Rechtsgutes und des Gefahrenstufe – befugt sein kann, auch solche »makelbehafteten« Informationen zu nutzen, um Gefahrenlagen aufzuklären.

Die Rechtslage, die im Detail allerdings nicht abschließend geklärt ist, wurde während der öffentlichen Sachverständigenanhörung im NSA-Untersuchungsausschuss diskutiert. Nach Ansicht der Sachverständigen dürfen die zuständigen Behörden solche Informationen im Falle einer konkreten und dringenden Gefahr für ein überragend wichtiges Gemeinschaftsgut oder für eine Vielzahl überragender individueller Rechtsgüter durchaus als Grundlage verwenden, um eigene Ermittlungen anzustellen.[96] Außerdem mache es einen Unterschied, ob der BND die Übermittlung selbst veranlasst habe, ob es sich gar um einen fortlaufenden Ringtausch von Informationen handle oder ob die Erkenntnisse spontan von einem gelegentlich kooperierenden Nachrichtendienst zur Verfügung gestellt worden seien.[97]

Keinesfalls darf der BND seine Grundrechtsbindung gezielt umgehen, indem er sich routinemäßig und anlasslos Informationen von ausländischen Diensten beschafft, die diese unter grundrechtswidrigen Bedingungen gewinnen und die der BND seinerseits auf diese Weise nicht gewinnen darf.[98] Auch ein zwischenstaatliches Abkommen über eine Kooperation der Nachrichtendienste könnte einen solchen Grundrechtsverstoß nicht legalisieren.

96 Mündliche Einlassung des Sachverständigen Papier im NSA-Untersuchungsausschuss, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, Stenographisches Protokoll der 5. Sitzung vom 22.5.2014, S. 45, 52; in diesem Sinne auch die mündlichen Einlassungen der Sachverständigen Hoffmann-Riem, ebd., S. 43, 50, und Bäcker, ebd., S. 49f.

97 Mündliche Einlassung des Sachverständigen Bäcker [wie Fn. 96], S. 42. Nach Ansicht des Sachverständigen müsse weiter differenziert werden: »Worin genau besteht das Problem aus Sicht des deutschen Rechts bei der Datenerhebung durch die ausländische Stelle? – Ich kann mir zum Beispiel ohne Weiteres vorstellen, dass eine ausländische Rechtsordnung den Gesetzesvorbehalt nicht mit der vollen Strenge durchzieht, wie wir das in Deutschland tun, wo wir ja für jede Eingriffsmaßnahme eine formell-gesetzliche Grundlage verlangen. Wenn jetzt eine ausländische Rechtsordnung diese Forderungen so nicht kennt, dafür aber sehr starke exekutive Schutzmechanismen vorsieht, die eben doch gewährleisten, dass eine Vorfestlegung erfolgt, die gleichzeitig auch zu Begrenzungen von Datenerhebungen führt, dann ist eine solche Datenübermittlung sicherlich grundrechtlich sehr viel weniger problematisch als wenn es um Daten geht, die zum Beispiel durch Folter erlangt worden sind.«

98 Dazu Wolfgang Ewer/Tobias Thienel, »Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals«, in: *Neue Juristische Wochenschrift*, 2014, S. 30–36 (35f).

Der gesetzliche Auftrag des BND und seine Befugnisse

Der BND ist eine Bundesoberbehörde im Geschäftsbereich des Bundeskanzleramtes.[99] Bis Ende der 1960er Jahre war der BND allein auf der Grundlage exekutiven Innenrechts tätig. Eine Regelung seiner Befugnisse durch Gesetz wurde nicht für erforderlich gehalten. Zum einen herrschte die Auffassung vor, dass die bloße Beschaffung von Informationen jenseits der Anwendung von Zwangsmaßnahmen (wozu der BND von Anfang an als nicht befugt galt) keinen Eingriff in Grundrechte darstelle. Zum anderen ging man davon aus, dass der BND überwiegend im Ausland aktiv werde, wo weder das Grundgesetz noch deutsche Befugnisnormen Geltung beanspruchen könnten.[100] Erst 1968 wurde im Zuge der Aufnahme der Notstandsverfassung in das Grundgesetz und der damit verbundenen Änderung von Art. 10 GG eine gesetzliche Basis für die Überwachung und Aufzeichnung von Telekommunikation geschaffen (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10-Gesetz, G 10).[101] Die zweite wichtige Rechtsquelle neben dem Artikel 10-Gesetz ist das BND-Gesetz von 1990.[102] Zudem finden sich in weiteren Gesetzen einzelne Sonderregelungen, die den BND betreffen.[103]

Rechtsquellen

Das Artikel 10-Gesetz stützt sich auf eine besondere Vorschrift im Grundgesetz (Art. 10 Abs. 2 S. 2 GG), wonach der Gesetzgeber zum Schutz der freiheitlichen demokratischen Grundordnung bzw. zur Sicherung des Bundes oder eines Bundeslandes Regelungen für besonders weitgehende Eingriffe in das Fernmeldegeheimnis schaffen kann.[104] Dementsprechend hoch sind die materiellen und formellen Voraussetzungen, unter denen der BND (ebenso wie die Verfassungsschutzbehörden des Bundes und der Länder sowie der Militärische Abschirmdienst) gemäß dem Artikel 10-Gesetz die Telekommunikation überwachen und aufzeichnen darf. Zum Beispiel sieht das Gesetz an bestimmten Stellen eine Beteiligung des Parlamentarischen Kontrollgremiums und der G 10-Kommission vor (zur Funktion beider Gremien im Zusammenhang mit der strategischen Fernmeldeaufklärung siehe S. 31); und es enthält spezielle Vorgaben für den Umgang mit den im Rahmen der Überwachung erhobenen personenbezogenen Daten (insbesondere strenge Zweckbindung der Verwendung und entsprechende Kennzeichnung der Daten, im Vergleich zum BND-Gesetz kürzere Prüfungsfristen bezüglich der Erforderlichkeit der gespeicherten Daten sowie besondere Voraussetzungen für die Übermittlung). Allerdings deckt das Artikel 10-Gesetz nicht das gesamte Spektrum der Telekommunikationsüberwachung ab. Darauf wird weiter unten noch ausführlicher einzugehen sein.

Auslöser dafür, dass es zum Erlass des BND-Gesetzes kam, war das Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983.[105] Wie das Gericht entschieden hatte, stellt die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Daten einen Eingriff in das Recht auf informationelle Selbstbestimmung dar und bedarf einer gesetzlichen Grundlage. Als Folge des Urteils wurde 1990 ein Gesetzespaket zur Fortentwicklung der Daten-

99 Im Jahr 1956 wurde die »Organisation Gehlen«, die sich nach Ende des Zweiten Weltkriegs aus ehemaligen Mitarbeitern von Aufklärungseinheiten der Wehrmacht gebildet hatte und unter amerikanischer Führung operierte, in den neu gegründeten BND überführt.

100 Gusy, »BND-Gesetz« [wie Fn. 91], S. 1262.

101 Ursprüngliche Fassung vom 13.8.1968 (BGBl. 1968 I S. 949). 1970 war das Artikel 10-Gesetz erstmals Gegenstand einer Überprüfung vor dem Bundesverfassungsgericht (BVerfGE 30, 1). Durch das Verbrechensbekämpfungsgesetz von 1994 wurde das Artikel 10-Gesetz grundlegend geändert, um der Bedrohung durch den internationalen Terrorismus und verschiedenen Formen der organisierten Kriminalität wirksamer begegnen zu können (BGBl. 1994 I, S. 3186). Im Zuge dieser Novellierung kam es zu einer erheblichen Erweiterung der Befugnisse des BND. Einzelne Bestimmungen dieser Novelle hat das Bundesverfassungsgericht 1999 für verfassungswidrig erklärt (BVerfGE 100, 313). Daraufhin wurde das Artikel 10-Gesetz im Jahr 2001 neu gefasst (BGBl. 2001 I, S. 1254 und 2298) und seitdem mehrfach geändert, zuletzt am 12.6.2015.

102 BGBl. 1990 I, S. 2954 (2979). Die aktuellste Änderung datiert vom 20.6.2013.

103 Übersicht bei Gusy, »BND-Gesetz« [wie Fn. 91], S. 1264.

104 Zu den Anforderungen an solche Regelungen siehe BVerfGE 30, 1 (27ff).

105 BVerfGE 65, 1.

verarbeitung und des Datenschutzes verabschiedet,[106] zu dem unter anderem auch das BND-Gesetz und das Bundesverfassungsschutzgesetz (BVerfSchG) gehörten. Beide Gesetze weisen eine systematische Verwandtschaft auf. Das Bundesverfassungsschutzgesetz ist jedoch deutlich umfangreicher und detaillierter und dient dem BND-Gesetz als Bezugsquelle. Wegen zahlreicher Verweisungen (über 20 zum Teil verschachtelte Verweisungen in 12 Paragraphen) lässt sich die Rechtslage nach dem BND-Gesetz nur mit großem Aufwand ermitteln. In der kommentierenden Literatur werden sowohl das BND-Gesetz als auch die dazu gehörige Gesetzesbegründung[107] wegen ihrer »apodiktischen Kürze« kritisiert. Diese Knappheit sei zum einen darauf zurückzuführen, dass der Text über die auslandsbezogenen Aufgaben und Aktivitäten des BND nicht mehr als unbedingt nötig offenlegen solle. Außerdem solle der Text des BND-Gesetzes offenbar auch über die möglichen Aufklärungsmaßnahmen nicht mehr als zwingend notwendig verraten.[108] Dementsprechend sind die Regelungen über die Aufgaben und Befugnisse des BND sehr allgemein gehalten und wenig aussagekräftig. Diese Regelungstechnik bringt ein relativ geringes Maß an Normenklarheit und Normenbestimmtheit mit sich, was unter verfassungsrechtlichen Gesichtspunkten problematisch ist (siehe unten S. 37).[109]

Auftrag

Die Aufgabe des BND besteht gemäß § 1 Abs. 2 S. 1 BNDG darin, zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen zu sammeln und auszuwerten. Sein Aufklärungsauftrag erstreckt sich somit ausschließlich auf Erkenntnisse »über das Ausland«. Sachverhalte, Personen und Vorgänge des politischen Geschehens *innerhalb* der Bundesrepublik – auch soweit das Geschehen von außen- und sicherheitspolitischer Bedeutung ist – sind nicht Gegenstand der nachrichtendienstlichen Aufklärung durch den BND.[110] Dies bedeutet nicht, dass der Raum, in dem der BND Informationen sammeln darf, auf das Ausland begrenzt ist. Zu Gewinnung von Erkenntnissen über das Ausland darf der BND auch im Bundesgebiet tätig werden.

Die zu gewinnenden Erkenntnisse müssen, wie erwähnt, »von außen- und sicherheitspolitischer Bedeutung« für Deutschland sein. Darunter fallen in erster Linie Erkenntnisse über bestimmte internationale Gefahrenlagen, die die Sicherheit Deutschlands beeinträchtigen. Das Artikel 10-Gesetz listet in § 5 einzelne Gefahrenbereiche auf, zu deren Aufklärung der BND internationale Telekommunikationsbeziehungen strategisch überwachen darf. Unter Beobachtung steht zum Beispiel die Lage in Gebieten, in denen die Bundeswehr eingesetzt ist. Allerdings beschränkt sich das Mandat des BND nicht auf die Gewinnung sicherheitsbedeutsamer Erkenntnisse; auch eine Konzentration auf Risiken oder rechtswidrige Vorgänge würde zu kurz greifen. Vielmehr geht es generell darum, Sachverhalte aufzuklären, die sich auf die Souveränität und Handlungsfähigkeit der Bundesrepublik auswirken können. Die Rahmenbedingungen, Optionen und möglichen Folgen eigenen außenpolitischen Handelns stehen ebenso im Fokus wie das Handeln anderer Staaten, internationaler Organisationen und nichtstaatlicher Akteure. Dazu zählen auch Erkenntnisse, die für die außenwirtschaftliche Betätigung der Bundesrepublik relevant sind, etwa Informationen über Versorgungssicherheit und die Sicherheit von Verkehrs- und Transportwegen im Ausland. Selbst die Belange deutscher Unternehmen im Ausland können in den Fokus des BND rücken, soweit sie von außen- und sicherheitspolitischer Bedeutung sind. Daraus ergibt sich für den BND insgesamt ein weites Tätigkeitsfeld.[111]

Die Prioritäten, nach denen der BND im Rahmen seines Auftrags Informationen sammeln und auswerten soll, werden von der Bundesregierung in einem Auftragsprofil festgelegt. Dieses Profil beschreibt verschiedene Themenbereiche, die für Deutschland von außen- und sicherheitspolitischer Bedeutung sind. Innerhalb des Profils genießt der BND jedoch Spielräume bei der Verteilung seiner Ressourcen und der Wahl seiner Mittel.[112] Über seine Tätigkeit hat der BND das Bundeskanzleramt zu unterrichten, das die

106 BGBl. 1990 I, S. 2954.
107 BR-Drs. 618/88.
108 Gusy, »BND-Gesetz« [wie Fn. 91], S. 1263f.
109 Dazu ebd., 1264. Siehe auch die Kritik von Markus Löning, *Eine Reformagenda für die deutschen Geheimdienste: rechtsstaatlich, demokratisch, effektiv*, Berlin: Stiftung Neue Verantwortung, April 2015 (Policy Brief), S. 3.
110 BR-Drs. 618/88, S. 183.
111 Gusy, »BND-Gesetz« [wie Fn. 91], S. 1270ff.
112 Graulich, *Nachrichtendienstliche Fernmeldeaufklärung* [wie Fn. 1], S. 39f.

rechtliche und politische Verantwortung für die Behörde trägt. Außerdem sind einzelne Bundesministerien im Rahmen ihrer Zuständigkeiten vom BND über relevante Erkenntnisse zu informieren (§ 12 BNDG).

Befugnisse nach dem BND-Gesetz

Die allgemeine Befugnisnorm zur Erhebung von Informationen einschließlich personenbezogener Daten im Bundesgebiet sowie zur Verarbeitung und Nutzung solcher Daten ist § 2 Abs. 1 BNDG.[113] Gemäß § 3 BNDG iVm § 9 Abs. 2 BVerfSchG darf der BND sogar das in einer Wohnung nichtöffentlich gesprochene Wort heimlich mithören und aufzeichnen; und er darf verdeckt technische Mittel einsetzen, um Bildaufnahmen und Bildaufzeichnungen anzufertigen. Solche Lausch- und Spähangriffe stellen schwerwiegende Eingriffe in die Privatsphäre und das durch Art. 13 GG garantierte Grundrecht auf Unverletzlichkeit der Wohnung dar. Sie unterliegen daher strengen Voraussetzungen.[114] Außerdem enthält § 9 Abs. 4 BVerfSchG die Befugnis zum Einsatz technischer Mittel, um den Standort aktiv geschalteter Mobilfunkendgeräte, die Gerätenummer oder Kartennummer zu ermitteln. Für die Durchführung von Online-Durchsuchungen[115] findet sich hingegen weder im BND-Gesetz noch im Bundesverfassungsschutzgesetz eine Ermächtigung. Nach Auskunft der Bundesregierung führt der BND daher im Inland sowie gegen deutsche Personen im Ausland keine Online-Durchsuchungen durch.[116]

Im Zusammenhang mit der Überwachung elektronischer Kommunikation ermächtigt das BND-Gesetz auch zur Erhebung von Bestandsdaten[117] und Verkehrsdaten (§§ 2a und 2b BNDG iVm §§ 8a ff BVerfSchG). Besondere Regelungen zur Verarbeitung und Nutzung personenbezogener Daten finden sich in den §§ 4 bis 6 und 8 bis 11 BNDG. Polizeiliche Zwangsbefugnisse stehen dem BND nicht zu, und er darf die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen er selbst nicht befugt ist (§ 2 Abs. 3 BNDG).

Befugnisse nach dem Artikel 10-Gesetz

Die generelle Befugnis des BND zur Überwachung und Aufzeichnung der Telekommunikation ergibt sich aus § 1 Abs. 1 G 10. Die Voraussetzungen, unter denen eine Überwachung zulässig ist, sind in drei Tatbeständen geregelt, die jeweils unterschiedliche Zwecke verfolgen: (1) die gezielte Überwachung einzelner Personen zur Abwehr bestimmter Gefahren[118] bei Vorliegen des Verdachts bestimmter Straftaten[119] (§ 3 G 10); (2) die

113 Gemäß § 2 Abs. 1 BNDG muss es sich entweder um Informationen über Vorgänge im Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, handeln; oder die Informationen müssen zur Eigensicherung und zum Quellenschutz, für die Sicherheitsüberprüfung von Personen, die für den BND tätig sind oder tätig werden sollen, oder für die Überprüfung von Nachrichtenzugängen erforderlich sein. Im erstgenannten Fall setzt die Zulässigkeit der Maßnahme voraus, dass die Informationen nur auf diese Weise zu erlangen sind und für ihre Erhebung keine andere Behörde zuständig ist.

114 Gemäß Art. 13 Abs. 4 S. 1 GG dürfen zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder Lebensgefahr, technische Mittel zur Überwachung von Wohnungen nur aufgrund richterlicher Anordnung eingesetzt werden. Bei Gefahr im Verzug kann die Maßnahme auch durch eine andere gesetzlich bestimmte Stelle angeordnet werden, wobei eine richterliche Entscheidung dann unverzüglich nachzuholen ist. Zu den Anforderungen siehe BVerfGE 109, 279. Umgesetzt werden diese Vorgaben durch § 9 Abs. 2 BVerfSchG.

115 Siehe dazu BVerfGE 120, 274.

116 BT-Drs. 17/1814, S. 4.

117 Bestandsdaten sind Daten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikations- oder Teledienste erhoben werden (§ 3 Nr. 3 TKG, § 8a Abs. 1 BVerfSchG).

118 Zur Abwehr drohender Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes, einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nato-Vertrages (§ 1 Abs. 1 Nr. 1 G 10).

119 Der abschließende Katalog des § 3 Abs. 1 G 10 umfasst Straftaten des Friedensverrats und Hochverrats; Straftaten der Gefährdung des demokratischen Rechtsstaates; Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit; Straftaten gegen die Landesverteidigung; Straftaten gegen die Sicherheit der in der Bundesrepublik stationierten Truppen der nichtdeutschen Vertragsstaaten des Nato-Vertrages; die Bildung terroristischer Vereinigungen; Volksverhetzung; verschiedene andere schwere Straftaten (Mord, Totschlag, erpresserischer Menschenraub, Geiselnahme, Brandstiftung, bestimmte Sprengstoffdelikte, qualifizierte gefährliche Eingriffe in den Bahn-, Schiffs- und Luftverkehr, besonders schwere Störung öffentlicher Betriebe und Angriffe auf den Luft- und Seeverkehr), soweit sie sich gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richten; sowie die Zugehörigkeit im Bundesgebiet zu einer überwiegend aus Ausländern bestehenden Vereinigung oder Gruppe, deren

strategische Überwachung internationaler Telekommunikationsbeziehungen zur Aufklärung oder Abwehr bestimmter Gefahrenlagen (§ 5 G 10); und (3) die strategische Überwachung zur Aufklärung oder Abwehr einer im Einzelfall bestehenden Gefahr für Leib oder Leben einer Person im Ausland, sofern die Belange der Bundesrepublik Deutschland unmittelbar in besonderer Weise berührt sind (§ 8 G 10). Bei all diesen Maßnahmen spricht das Gesetz allgemein von »Beschränkungen«.

Bestehen, Zielsetzung oder Tätigkeit vor den Behörden geheim gehalten wird, um ihr Verbot abzuwenden (§ 95 Abs. 1 Nr. 8 des Aufenthaltsgesetzes).

Strategische Überwachung internationaler Telekommunikation durch den BND

Die Rechtsgrundlage für eine strategische Überwachung internationaler Telekommunikation ist § 5 G 10. Allerdings vertritt die Bundesregierung die Position, dass im Anwendungsbereich von § 5 G 10 nur Verkehre von Deutschland ins Ausland bzw. aus dem Ausland nach Deutschland erfasst werden.[120] Die Überwachung und Aufzeichnung von Kommunikationsverkehren, bei denen sich beide Teilnehmer im Ausland befinden – BND-intern hat sich dafür die Bezeichnung »Routineverkehre« durchgesetzt[121] – erfolgt nach dieser Lesart außerhalb des Artikel 10-Gesetzes.

Strategische Überwachung nach § 5 G 10 (Deutschland-Ausland)

Gemäß § 5 Abs. 1 G 10 darf eine strategische Überwachung und Aufzeichnung internationaler Telekommunikationsbeziehungen angeordnet werden, um Informationen über Sachverhalte zu sammeln, deren Kenntnis notwendig ist, um bestimmte Gefahren[122] rechtzeitig zu erkennen oder ihnen zu begegnen. Anders als bei der gezielten Einzelüberwachung nach § 3 G 10 (dort werden tatsächliche Anhaltspunkte für den Verdacht der Planung oder Begehung bestimmter Straftaten[123] gefordert) und anders als im Strafprozessrecht oder Polizeirecht, existiert für die strategische Fernmeldeaufklärung nach § 5 G 10 keine besondere Eingriffsschwelle, d.h. es muss beispielsweise keine der genannten Gefahren bereits konkret vorliegen. Ausreichend ist, dass bei Durchführung der Überwachungsmaßnahme Erkenntnisse über bestehende Gefahrenlagen zu erwarten sind.[124]

Wichtig ist die Begrenzung der Überwachungsbefugnisse nach § 5 G 10 auf die *internationale* Telekommunikation. Nur wenn sich mindestens einer der Teilnehmer im Ausland befindet, darf die Kommunikation überwacht und aufgezeichnet werden. Rein innerdeutsche Kommunikationsverkehre zwischen Teilnehmern im Bundesgebiet sind von der strategischen Fernmeldeaufklärung ausgenommen.[125] Da es vorkommt, dass Inlandsverkehre über Leitungen im Ausland abgewickelt werden, die vom BND überwacht werden, verwendet dieser Systeme, mit denen solche Verkehre automatisch herausgefiltert werden sollen, ohne dass eine Erfassung oder Speicherung erfolgt.[126] In diesem Zusammenhang hat das Bundesverfassungsgericht entschieden, dass es an einem Eingriff in das Fernmeldegeheimnis nach Art. 10 GG jedenfalls dann fehlt, wenn Fernmeldevorgänge zwischen deutschen Anschlüssen ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Signalaufbereitung technisch wieder spurenlos ausgesondert werden.[127]

120 BT-Drs. 17/9640, S. 6; 17/14739, S. 14. Siehe auch die Gesetzesbegründung von 2001 (BT-Drs. 14/5655, S. 18). Dazu Bäcker, *Stellungnahme zur Anhörung* [wie Fn. 80], S. 16f; Huber, »Artikel 10-Gesetz« [wie Fn. 77], S. 1354.

121 Im Zusammenhang mit der Überwachung des nichtleitungsgebundenen Fernmeldeverkehrs wird auch von einer Überwachung des »offenen Himmels« gesprochen.

122 § 5 Abs. 1 S. 3 G 10 bezieht sich auf die Gefahr (1) eines bewaffneten Angriffs auf die Bundesrepublik Deutschland; (2) internationaler terroristischer Anschläge mit unmittelbarem Bezug zu Deutschland; (3) der internationalen Verbreitung von Kriegswaffen und des unerlaubten Außenwirtschaftsverkehrs mit Waren, Datenverarbeitungsprogrammen und Technologien in Fällen von erheblicher Bedeutung; (4) der unbefugten gewerbs- oder bandenmäßig organisierten Verbringung von Betäubungsmitteln in das Gebiet der EU in Fällen von erheblicher Bedeutung mit Bezug zu Deutschland; (5) der Beeinträchtigung der Geldwertstabilität im Euro-Währungsraum durch im Ausland begangene Geldfälschungen; (6) der international organisierten Geldwäsche in Fällen von erheblicher Bedeutung; (7) des gewerbs- oder bandenmäßig organisierten Einschleusens ausländischer Personen in das Gebiet der EU in Fällen von erheblicher Bedeutung mit Bezug zu Deutschland, und zwar (a) bei unmittelbarem Bezug zu den drei erstgenannten Gefahrenbereichen (bewaffneter Angriff, Terrorismus, Proliferation); (b) in Fällen, in denen eine erhebliche Anzahl geschleuster Personen betroffen ist, vor allem wenn durch die Art der Schleusung von einer Gefahr für ihr Leib oder Leben auszugehen ist; oder (c) in Fällen, in denen das Einschleusen durch ausländische öffentliche Stellen unmittelbar oder mittelbar unterstützt oder geduldet wird.

123 Siehe Fn. 119.

124 BVerwGE 130, 180 (Rn. 29). Siehe auch BVerfGE 100, 313 (383). Bäcker, *Stellungnahme zur Anhörung* [wie Fn. 80], kritisiert, dass § 5 Abs. 1 G 10 hinsichtlich der meisten Gefahrenbereiche eine permanente Überwachungstätigkeit ermögliche, da stets mit entsprechenden Gefährdungen zu rechnen sei.

125 Huber, »Artikel 10-Gesetz« [wie Fn. 77], S. 1394.

126 BT-Drs. 17/14739, S. 14.

127 BVerfGE 100, 313 (366). Dazu, wie der BND die Grenze

Anordnung

Welche internationalen Telekommunikationsbeziehungen im Zusammenhang mit einem bestimmten Gefahrenbereich jeweils überwacht werden sollen, wird auf Antrag des BND vom Bundesministerium des Innern (Art. 10 Abs. 1 G 10)[128] mit Zustimmung des Parlamentarischen Kontrollgremiums angeordnet. Die Überwachung darf höchstens drei Monate dauern, wobei Verlängerungen um jeweils nicht mehr als drei weitere Monate möglich sind. Die Parameter der Überwachung, die in der Anordnung fixiert sein müssen, gibt § 10 Abs. 4 G 10 vor. Erstens ist das geographische Gebiet festzulegen, über das Informationen gesammelt werden sollen. In der Regel handelt es sich dabei um das Territorium eines oder mehrerer Staaten oder um eine bestimmte Region (z.B. Afghanistan/Pakistan). Zweitens müssen die zu überwachenden Übertragungswege bezeichnet werden (z.B. Kabelverbindung von A nach B; Übertragungsweg X des Satelliten Y).[129] Drittens ist festzulegen, welcher Anteil der auf dem jeweiligen Übertragungsweg zur Verfügung stehenden Übertragungskapazität überwacht werden soll. Dieser Anteil darf nicht mehr als 20 Prozent betragen. Dadurch soll einer lückenlosen Überwachung vorgebeugt und der strategische Charakter der Maßnahme bewahrt werden. Angesichts dieser Begrenzungen hat das Bundesverwaltungsgericht strategischen Beschränkungen nach § 5 G 10 lediglich »fragmentarischen Charakter« beigemessen.[130] Kritisiert wird aber, dass diese Quote bei mangelnder Auslastung der Übertragungswege offenbar keine effektive Begrenzung darstellt.[131] Viertens müssen auch die Suchbegriffe, die bei der Überwachung verwendet werden sollen, in der Anordnung aufgelistet sein.

Zugriff

Wie der BND bei der strategischen Telekommunikationsüberwachung vorgeht, lässt sich anhand der öffentlich zugänglichen Quellen nur in groben Umrissen nachvollziehen.[132] Zunächst muss ein Zugang zu den jeweiligen Übertragungswegen geschaffen werden. Daher verpflichtet § 2 G 10 die Anbieter von Telekommunikationsdienstleistungen dazu, dem BND die Überwachung und Aufzeichnung der Kommunikation zu ermöglichen. Einzelheiten sind im Telekommunikationsgesetz (TKG) und in der Telekommunikations-Überwachungsverordnung (TKÜV) geregelt.[133] Voraussetzung ist eine Anordnung nach § 5 G 10. Die gesetzlichen Zugriffsbefugnisse gelten selbstverständlich nur innerhalb des Hoheitsbereichs der Bundesrepublik. Im Ausland hat der BND keine rechtliche Handhabe, um sich entsprechenden Zugang zu verschaffen. Prinzipiell ist aber auch denkbar, dass Zugriffsrechte zugunsten des BND in einem öffentlich-rechtlichen Vertrag mit dem Betreiber geregelt werden.

zwischen Datenerfassung und Grundrechtseingriff zieht, siehe die Vernehmung des Zeugen A. F. [wie Fn. 57], S. 116f.

128 Zur Vorgängerregelung siehe Huber, »Artikel 10-Gesetz« [wie Fn. 77], S. 1424. Siehe auch § 2a BNDG, wonach für Anordnungen im Zusammenhang mit besonderen Auskunftsverlangen über Bestandsdaten und Verkehrsdaten das Bundeskanzleramt zuständig ist.

129 BT-Drs. 14/5655, S. 23.

130 Bundesverwaltungsgericht, Urteil vom 28.05.2014 (6 A 1.13), Rn. 29.

131 Bäcker, *Stellungnahme zur Anhörung* [wie Fn. 80], S. 12f.

132 Die Bundesregierung nimmt in ihren Antworten auf Kleine Anfragen von Bundestagsfraktionen regelmäßig nur oberflächlich zu den Abläufen öffentlich Stellung. Die meisten Informationen sind als »VS-Vertraulich« oder »VS-Geheim« eingestuft. Das ist immer dann der Fall, wenn die Antwort nach Auffassung der Bundesregierung operative Details betrifft, deren Offenlegung die Auftragserfüllung des BND und mithin die Sicherheit der Bundesrepublik beeinträchtigen könnte. Die Antworten werden dann je nach Einstufung entweder dem Bundestag zur Einsichtnahme übermittelt oder in dessen Geheimschutzstelle hinterlegt. Zur Veranschaulichung der Praxis und der Rechtsauffassung des BND kann vor allem auf die Aussagen von aktuellen und ehemaligen BND-Mitarbeitern verwiesen werden, die vor dem NSA-Untersuchungsausschuss als Zeugen ausgesagt haben (siehe Fn. 57). Weitere Einblicke ergeben sich aus dem Bericht von Graulich, *Nachrichtendienstliche Fernmeldeaufklärung* [wie Fn. 1].

133 Im Falle der Fernmeldeaufklärung internationaler leitungsgebundener Telekommunikation sind die Betreiber der jeweiligen Telekommunikationsanlagen unter anderem dazu verpflichtet, dem BND an einem bestimmten Übergabepunkt eine vollständige Kopie der Telekommunikation bereitzustellen, die auf den in der Anordnung bezeichneten Wegen übertragen wird. Außerdem hat der Betreiber in seinen Räumen die Aufstellung und den Betrieb von Geräten des BND zu dulden (§ 110 TKG iVm §§ 26ff TKÜV).

G 10-Filter

Ein zentrales Element der strategischen Überwachung nach § 5 G 10 ist die Trennung zwischen Kommunikationsverkehren, die dem Schutz von Art. 10 GG unterliegen (und deren Überwachung damit den strengen Vorgaben des Artikel 10-Gesetzes folgen muss), und solchen, die nicht durch Art. 10 GG geschützt sind (und die unter weniger strengen Vorgaben überwacht werden). Für diese Trennung verwendet der BND ebenfalls spezielle Filter. In Zweifelsfällen wird die Prüfung von einzelnen Mitarbeitern durch zusätzliche Recherchen »per Hand« vorgenommen.[134]

Der BND geht davon aus, dass es sich dann um einen G 10-Verkehr handelt, wenn mindestens einer der Teilnehmer durch Art. 10 GG geschützt ist.[135] Die Beantwortung der Frage, ob ein Kommunikationsverkehr unter dieses Kriterium fällt, hängt davon ab, wie man den personalen und räumlichen Schutzbereich des Fernmeldegeheimnisses definiert. Konkret geht es darum, wer zum Kreis der Grundrechtsberechtigten zählt und wie weit die Grundrechtsbindung des Staates reicht (siehe oben, S. 17 und 18). In einem Bericht von Oktober 2015 hat der ehemalige Richter am Bundesverwaltungsgericht Dr. Kurt Graulich im Auftrag des NSA-Untersuchungsausschusses das Rechtsverständnis und die Rechtspraxis des BND zu diesen Fragen zusammengefasst.[136] Danach schütze Art. 10 GG im Inland das Fernmeldegeheimnis aller natürlichen Personen unabhängig von ihrer Staatsangehörigkeit sowie bestimmte inländische juristische Personen des Privatrechts und einige wenige juristische Personen des öffentlichen Rechts. Im Ausland seien deutsche Staatsangehörige und Tochterunternehmen inländischer juristischer Personen ebenfalls geschützt. Nicht in den Schutzbereich von Art. 10 GG fielen hingegen ausländische juristische Personen sowie Ausländer im Ausland.[137]

Darüber hinaus schildert Graulich die sogenannte »Funktionsträgertheorie«, die offenbar Teil der Rechtsauffassung des BND ist. Nach dieser Theorie wird das Handeln einer natürlichen Person (zum Beispiel des Geschäftsführers einer GmbH) unmittelbar der dahinterstehenden juristischen Person zugerechnet. Folglich sei der nichtdeutsche Mitarbeiter eines deutschen Unternehmens, wenn er in einer Niederlassung im Ausland im Rahmen seiner Funktion telefoniere, vom G 10-Schutz des Unternehmens miterfasst.[138] Daraus lässt sich umgekehrt aber auch der Schluss ziehen, dass deutsche Staatsangehörige, die für eine ausländische juristische Person tätig sind und in dieser Funktion für die juristische Person kommunizieren, gerade nicht durch Art. 10 GG geschützt sind.[139] Eine solche einschränkende Auslegung des personalen und räumlichen Schutzbereichs des Fernmeldegeheimnisses lässt sich mit der herrschenden Grundrechtslehre allerdings nur schwer vereinbaren (siehe oben, S. 17 und 18).

Selektion und Auswertung

Nach der Filterung werden diejenigen Kommunikationsverkehre, die unter § 5 G 10 fallen, gemäß Absatz 2 dieser Vorschrift anhand von G 10-konformen Suchbegriffsprofilen gescannt. Welche Suchbegriffe zum Einsatz kommen, ergibt sich aus der jeweiligen Anordnung. § 5 Abs. 2 G 10 schränkt die Auswahl möglicher Suchbegriffe in dreierlei Hinsicht ein. Erstens müssen die Suchbegriffe zur Aufklärung von Sachverhalten im Zusammenhang mit dem in der jeweiligen Anordnung bezeichneten Gefahrenbereich »bestimmt und geeignet« sein. Zweitens dürfen keine Suchbegriffe mit Identifizierungsmerkmalen verwendet werden, die zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen.[140] Und drittens ist es

134 Filterkriterien sind etwa Telefon- und Faxvorwahlen (z.B. +49 für Deutschland) oder Top-Level-Domains von Websites (z.B. [...].de). Gegebenenfalls wird im Einzelfall speziell geprüft, ob es sich bei einem Kommunikationsteilnehmer tatsächlich um eine Person handelt, die durch Art. 10 GG geschützt ist. Die Genauigkeit und Verlässlichkeit solcher Filter lässt sich jedoch hinterfragen.

135 Siehe die Vernehmung des Zeugen Burbaum [wie Fn. 72], S. 18.

136 Graulich, *Nachrichtendienstliche Fernmeldeaufklärung* [wie Fn. 1], S. 42ff.

137 Ebd., S. 44. Siehe dazu auch die Vernehmung des Zeugen Burbaum [wie Fn. 72], S. 31.

138 Graulich, *Nachrichtendienstliche Fernmeldeaufklärung* [wie Fn. 1], S. 44.

139 Siehe die Vernehmung des Zeugen Burbaum [wie Fn. 72], S. 45ff, 64.

140 Dadurch soll verhindert werden, dass strategische Überwachungsmaßnahmen genutzt werden, um mehrere einzelne Anschlüsse in gebündelter Form zu kontrollieren. Das Bundesverfassungsgericht hat diesem Verbot im Hinblick auf den Grundsatz der Verhältnismäßigkeit besondere Bedeutung beigemessen, BVerfGE 100, 313 (384). Problematisch ist unter anderem aber, dass das Verbot in Bezug auf E-Mail-Postfächer praktisch leerläuft, da diese nicht an einen bestimmten Anschluss gekoppelt sind, sondern über die E-Mail-Adresse von jedem beliebigen Anschluss aufgerufen

verboten, Suchbegriffe zu verwenden, die den Kernbereich privater Lebensgestaltung[141] betreffen.

Die beiden zuletzt genannten Verbote gelten jedoch nicht für die strategische Überwachung von Telekommunikationsanschlüssen im Ausland, »sofern ausgeschlossen werden kann, dass Anschlüsse, deren Inhaber oder regelmäßige Nutzer deutsche Staatsangehörige sind, gezielt erfasst werden« (§ 5 Abs. 2 S. 3 G 10). Das Anliegen dieser Vorschrift besteht darin, deutsche Staatsangehörige zu schützen.[142] Vereinfacht ausgedrückt bedeutet das: Anschlüsse von Ausländern im Ausland dürfen sehr wohl mit Hilfe bestimmter Suchkriterien gezielt erfasst werden; und es dürfen in solchen Fällen auch Suchbegriffe verwendet werden, die den Kernbereich privater Lebensführung betreffen.[143] Die herrschende Grundrechtslehre geht allerdings davon aus, dass auch Ausländer im Ausland – soweit sie dort von der deutschen öffentlichen Gewalt betroffen sind – den Schutz derjenigen Grundrechte genießen, die nicht speziell als Deutschengrundrechte ausgestaltet sind (siehe oben, S. 20). Daher wird die Ausnahmeregelung des § 5 Abs. 2 S. 3 G 10 wegen ihrer Differenzierung zwischen deutschen und ausländischen Staatsangehörigen vielfach als verfassungswidrig kritisiert.[144]

Sind im Rahmen der Überwachung tatsächlich Kommunikationsinhalte aus dem Kernbereich privater Lebensgestaltung miterfasst worden, so dürfen diese jedenfalls nicht verwertet werden. Solche Inhalte sind unverzüglich zu löschen, es sei denn, es geht um die Gefahr eines bewaffneten Angriffs auf die Bundesrepublik (§ 5a G 10). Dieses Verwertungsverbot unterscheidet, anders als die Vorgaben zur Verwendung von Suchbegriffen, nicht zwischen Deutschen und Ausländern.

Kommunikationsverkehre, in denen kein Suchbegriff vorkommt, werden nicht gespeichert. Solche, in denen ein Suchbegriff enthalten ist, werden in mehreren Kaskaden automatisch[145] bzw. »per Hand« auf ihre Relevanz für den jeweiligen Überwachungsauftrag untersucht. Am Ende der Auswertungsphase werden die gewonnenen Informationen als Meldungen verarbeitet und den jeweils zuständigen Stellen der Regierung zugeleitet. Zudem wird geprüft, ob gegebenenfalls eine Übermittlung an andere Behörden oder ausländische Nachrichtendienste in Betracht kommt.[146] Nicht relevante Verkehre sind rückstandsfrei zu löschen.

Kontrolle

Die Bundesregierung unterliegt hinsichtlich der Tätigkeit des BND generell der Kontrolle durch das Parlamentarische Kontrollgremium, das sich aus Mitgliedern des Deutschen Bundestages zusammensetzt (Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes, PKGrG). Soweit es speziell um strategische Beschränkungen nach § 5 G 10 geht, ist das Bundesministerium des Innern bei der Festlegung der jeweils zu überwachenden Telekommunikationsbeziehungen an die Zustimmung des Parlamentarischen Kontrollgremiums gebunden. Dementsprechend wird das Gremium vom Bundesinnenministerium in Abständen von höchstens sechs Monaten über die Durchführung des Artikel 10-Gesetzes unterrichtet, und es muss dem Bundestag darüber jährlich Bericht erstatten (§ 14 G 10).[147]

Darüber hinaus prüft die G 10-Kommission regelmäßig die Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen, die nach dem Artikel 10-Gesetz getroffen werden (§ 15 G 10). Diese Prüfung, die von Amts wegen, aber auch aufgrund von Beschwerden erfolgt, soll das Fehlen gerichtlicher Kontrollmöglichkeiten kompensieren (siehe Art. 10 Abs. 2 GG). Die Mitglieder der Kommission werden vom Parlamentarischen Kontrollgremium bestellt und sind in ihrer Amtsführung unabhängig. Gegenstand der Prüfung ist unter anderem die Zulässigkeit der im Antrag be-

werden können, Bäcker, Stellungnahme zur Anhörung [wie Fn. 80], S. 14.

141 Siehe oben, S. 14.

142 BT-Drs. 14/5655, S. 20.

143 Siehe dazu BT-Drs. 16/12448, S. 11.

144 Bäcker, *Stellungnahme zur Anhörung* [wie Fn. 80], S. 14f mwN; Huber, »Artikel 10-Gesetz« [wie Fn. 77], S. 1402 mwN; Fredrik Roggan, *G 10-Gesetz*, Nomos Online-Kommentar, Baden-Baden 2012, § 5, Rn. 22; Papier, Interview, *Süddeutsche Zeitung* [wie Fn. 69]. Darüber hinaus wird von den Kommentatoren auch die Vereinbarkeit dieser Vorschrift mit der EMRK bezweifelt (Huber, ebd.).

145 Zur Prüfung der Relevanz kann auf Antrag ein Metadatenabgleich erfolgen (§ 6 Abs. 3 G 10). Dies bedeutet, dass die erhobenen Daten in einem automatisierten Verfahren mit bereits vorliegenden Rufnummern oder anderen Kennungen bestimmter Anschlüsse abgeglichen werden, bei denen tatsächliche Anhaltspunkte dafür bestehen, dass sie ihrerseits in einem Zusammenhang mit dem Gefahrenbereich stehen, auf den sich die aktuelle Überwachung bezieht. Siehe BT-Drs. 16/509, S. 9.

146 BT-Drs. 17/9640, S. 7, 8.

147 Die Berichte des Parlamentarischen Kontrollgremiums finden sich unter <www.bundestag.de/bundestag/gremien18/pkgr> (Zugriff am 12.4.2016).

nannten Suchbegriffe nach § 5 Abs. 2 G 10.[148] Im Übrigen erstreckt sich die Kontrollbefugnis der G 10-Kommission auf die gesamte Erhebung, Verarbeitung und Nutzung der nach dem Artikel 10-Gesetz erlangten personenbezogenen Daten einschließlich der Entscheidung darüber, ob die jeweiligen Maßnahmen dem Betroffenen im Nachhinein mitzuteilen sind.[149]

Die Kommission wird monatlich vom Bundesministerium des Innern über die angeordneten Maßnahmen unterrichtet; sie tritt mindestens einmal im Monat zusammen, um die einzelnen Anträge abzuarbeiten. In der Regel erfolgt die Prüfung durch die Kommission vor Vollzug der jeweiligen Beschränkungsmaßnahme. Bei Gefahr im Verzug kann das Bundesinnenministerium den Vollzug der Maßnahme jedoch bereits vor Unterrichtung der Kommission anordnen und die Bestätigung nachholen. Anordnungen, die die G 10-Kommission für unzulässig oder nicht notwendig erklärt, hat das Ministerium unverzüglich aufzuheben (§ 15 Abs. 6 S. 3 G 10).

Strategische Überwachung der Ausland-Ausland-Kommunikation und Umgang mit »Routineverkehren«

Im vorigen Abschnitt wurde darauf hingewiesen, dass § 5 G 10 nach Ansicht der Bundesregierung nur für die Überwachung und Aufzeichnung von Kommunikationsverkehren gilt, die von Deutschland ins Ausland bzw. aus dem Ausland nach Deutschland geführt werden.[150] Unklar ist, auf welcher Rechtsgrundlage Ausland-Ausland-Kommunikation überwacht wird bzw. nach welchen Vorgaben mit Kommunikationsverkehren verfahren wird, die im Falle einer Überwachung nach § 5 G 10 durch die Filterung als »Routineverkehre« identifiziert werden. Solche »Routineverkehre« werden in einem separaten Strang offenbar ebenfalls anhand von Selektoren gescannt und auf ihre nachrichtendienstliche Relevanz überprüft.[151] Im Artikel 10-Gesetz findet sich dafür aber keine Regelung. Daher greifen insoweit auch die von dem Gesetz vorgesehenen Kontrollmechanismen nicht.[152]

Der BND scheint sich bei der Überwachung der Ausland-Ausland-Kommunikation auf § 1 Abs. 2 S. 1 BNDG zu stützen.[153] Dabei handelt es sich jedoch nur um eine allgemeine Aufgabenzuweisung, nicht um eine Befugnisnorm.[154] Eine allgemeine Aufgabenzuweisung reicht nicht aus, um Grundrechtseingriffe zu rechtfertigen. Geht man davon aus, dass es auch bei der Überwachung und Aufzeichnung der Ausland-Ausland-Kommunikation zu Eingriffen in das Fernmeldegeheimnis nach Art. 10 GG kommt (siehe oben, S. 17 und 18), so bedarf es einer gesetzlichen Grundlage, die Anlass, Zweck und Grenzen des Eingriffs bereichsspezifisch, präzise und klar festlegt und dem Grundsatz der Verhältnismäßigkeit genügt.[155] Auch die generelle Befugnisnorm des § 2 Abs. 1 BNDG erfüllt die beschriebenen Voraussetzungen nicht.[156] Gemäß dieser Regelung darf der BND zu bestimmten Zwecken die erforderlichen Informationen einschließlich personenbezogener Daten erheben, verarbeiten und nutzen. Danach lassen sich zwar Eingriffe in das Grundrecht auf informationelle Selbstbestimmung rechtfertigen; Beschränkungen des Fernmeldegeheimnisses deckt § 2 Abs. 1 BNDG aber nicht ab. Dazu bedarf es einer speziellen Regelung wie in § 5 G 10.[157] Theoretisch ließe sich § 5 G 10 sogar unmittelbar auf die Überwachung der Ausland-Ausland-Kommunikation

148 Zum Umfang der Kontrolle durch die G 10-Kommission siehe Bundesverwaltungsgericht, Urteil vom 28.5.2014 [wie Fn. 130], Rn. 40f.

149 Die Mitteilung an Betroffene ist in § 12 G 10 geregelt. Zu den Defiziten dieser Regelung siehe Bertolt Huber, »Die strategische Rasterfahndung des Bundesnachrichtendienstes. Eingriffsbefugnisse und Regelungsdefizite«, in: *Neue Juristische Wochenschrift*, 2013, S. 2572–2577 (2574f).

150 Siehe Fn. 120.

151 Siehe die Vernehmung des Zeugen Burbaum [wie Fn. 72], S. 22.

152 Jürgen Seifert, »Die elektronische Aufklärung des Bundesnachrichtendienstes (BND). Zur unterschiedlichen Behandlung der elektronischen Ausland-Ausland-Aufklärung des BND und der elektronischen Aufklärung Ausland-Bundesrepublik nach § 5 G 10 Gesetz«, in: Bernd M. Kraske (Hg.), *Pflicht und Verantwortung. Festschrift zum 75. Geburtstag von Claus Arndt*, Baden-Baden 2002, S. 175–184 (181).

153 BT-Drs. 17/9640, S. 10. Siehe auch die Darstellung der Rechtsauffassung des BND in BVerfGE 100, 313 (380).

154 Die Vorschrift lautet: »Der Bundesnachrichtendienst sammelt zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus.« Dazu Bäcker, *Stellungnahme zur Anhörung* [wie Fn. 80], S. 18ff.

155 BVerfGE 110, 33 (53). Siehe oben, S. 13.

156 Huber, »Artikel 10-Gesetz« [wie Fn. 77], S. 1355.

157 Eine gesetzliche Vorschrift, durch die ein Grundrecht eingeschränkt wird, muss das betreffende Grundrecht unter Angabe des Artikels nennen (Art. 19 Abs. 1 S. 2 GG). Auch diese Voraussetzung erfüllt § 2 Abs. 1 BNDG nicht, soweit es um einen möglichen Eingriff in das Fernmeldegeheimnis geht.

anwenden. Der Gesetzeswortlaut stünde dem jedenfalls nicht entgegen.

Im Übrigen ist es durchaus relevant, ob Ausland-Ausland-Kommunikation gewissermaßen als »Beifang« auf der Grundlage einer Anordnung nach § 5 G 10 miterfasst und ausgewertet wird (ausgefiltert und jenseits der Vorgaben des Artikel 10-Gesetzes) oder ob solche Überwachungsmaßnahmen separat (ohne G 10-Anordnung) erfolgen. Im ersten Fall bietet die vom Bundesministerium des Innern mit Zustimmung des Parlamentarischen Kontrollgremiums erlassene Anordnung dem BND nämlich gemäß § 2 G 10 eine rechtliche Handhabe, um sich überhaupt bei den Betreibern der Telekommunikationsanlagen Zugriff auf die jeweiligen Kabelverbindungen zu verschaffen (siehe oben, S. 29). Bei Überwachungsmaßnahmen, die von vornherein außerhalb des Artikel 10-Gesetzes stattfinden, greift diese Vorschrift nicht. In diesen Fällen bliebe nur die Möglichkeit eines öffentlich-rechtlichen Vertrages mit dem jeweiligen Betreiber.

Übermittlung personenbezogener Daten an ausländische Nachrichtendienste

Die Auffassung, dass Ausländer im Ausland nicht durch Art. 10 GG geschützt sind und die strategische Überwachung und Aufzeichnung rein ausländischer Telekommunikationsverkehre nicht unter § 5 G 10 fällt, wirkt sich auch auf die Beantwortung der Frage aus, nach welchen Rechtsvorschriften die auf diesem Wege gewonnenen personenbezogenen Daten an ausländische Nachrichtendienste übermittelt werden dürfen.

Übermittlung nach dem Artikel 10-Gesetz

Das Artikel 10-Gesetz enthält bereichsspezifische Regelungen zum Datenschutz, die wegen der besonderen Schwere des Eingriffs ein relativ hohes Schutzniveau gewährleisten. Für den Umgang mit personenbezogenen Daten, die im Rahmen der strategischen Überwachung nach § 5 G 10 erhoben werden, gelten die §§ 6, 7 und 7a G 10. Diese Regelungen gehen sowohl den allgemeineren Regelungen des Bundesdatenschutzgesetzes (§ 1 Abs. 3 BDSG) als auch den datenschutzrechtlichen Regelungen des BND-Gesetzes vor.

Gemäß § 7a Abs. 1 G 10 dürfen an ausländische öffentliche Stellen überhaupt nur solche Daten übermittelt werden, die erhoben wurden, um der Gefahr internationaler terroristischer Anschläge, der Gefahr internationaler Proliferation oder der Gefahr des organisierten Einschleusens ausländischer Personen zu begegnen. In diesen Fällen ist eine Übermittlung zulässig, sofern drei Voraussetzungen erfüllt sind. Erstens muss die Übermittlung zur Wahrung außen- oder sicherheitspolitischer Belange der Bundesrepublik oder erheblicher Sicherheitsinteressen des Empfängerstaates erforderlich sein;[158] zweitens dürfen überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen;[159] und drittens muss das Prinzip der Gegenseitigkeit gewahrt sein. Hinter dem letzten Punkt steht der Gedanke, dass nur Staaten, die die Bundesrepublik an den Erkenntnissen ihrer eigenen Fernmeldeaufklärung teilhaben lassen, von der Telekommunikationsüberwachung durch den BND profitieren sollen.[160] Auch eine Übermittlung an Dienststellen der in Deutschland stationierten Nato-Streitkräfte ist unter gewissen Voraussetzungen zulässig (§ 7a Abs. 2 G 10).

Diejenige Person, die im BND über die Übermittlung entscheidet, muss die Befähigung zum Richteramt haben. Außerdem bedarf die Übermittlung der Zustimmung durch das Bundeskanzleramt. In jedem Fall ist der Empfänger zu verpflichten, die übermittelten Daten nur zu dem Zweck zu verwenden, zu dem sie ihm übermittelt wurden. Darüber hinaus muss er verpflichtet werden, eine an den Daten angebrachte Kennzeichnung beizubehalten und dem BND auf Ersuchen Auskunft über die Verwendung zu erteilen (§ 7a Abs. 4 G 10). Diese Vorgaben sind deutlich strikter formuliert als die vergleichbaren Passagen, die nach dem BND-Gesetz für die Übermittlung personenbezogener Daten gelten (dazu im folgenden Abschnitt). Denkbar sind beispielsweise Absprachen zwischen befreundeten Nachrichtendiensten, die eine solche Zweckbindung und diesbezügliche Auskünfte vorsehen. Insoweit kommt bis zu einem gewissen Grad sicherlich das gegenseitige Interesse an einem funktionierenden Datenaustausch als Motivationsfaktor zum Tragen. Tatsächlich dürften die Möglichkeiten des BND, die Zweckbindung durchzusetzen, allerdings relativ beschränkt sein.

Offen bleibt, auf welcher Rechtsgrundlage jene personenbezogenen Telekommunikationsdaten aus »Routineverkehren«, die entweder als »Beifang« im Rahmen der Überwachung nach § 5 G 10 oder gänzlich außerhalb dieses Rahmens gewonnen werden, an

158 Siehe dazu BT-Drs. 16/509, S. 10.

159 Die Übermittlung ist zulässig, soweit »insbesondere in dem ausländischen Staat ein angemessenes Datenschutzniveau gewährleistet ist sowie davon auszugehen ist, dass die Verwendung der Daten durch den Empfänger in Einklang mit grundlegenden rechtsstaatlichen Prinzipien erfolgt« (§ 7a Abs. 1 S. 1 Nr. 2 G 10). Zum Kriterium eines angemessenen Datenschutzniveaus vgl. § 4b Abs. 2 und 3 BDSG. Laut Gesetzesbegründung könne eine Übermittlung an einen ausländischen Staat ohne vergleichbares Datenschutzniveau jedoch dann in Frage kommen, wenn das Interesse an einer Übermittlung, zum Beispiel wegen einer erheblichen Gefahr für Leben oder Gesundheit von Menschen im Empfängerstaat, die schutzwürdigen Interessen des Betroffenen überwiege (BT-Drs. 16/509, S. 10).

160 BT-Drs. 16/509, S. 10.

ausländische Nachrichtendienste übermittelt werden dürfen.[161] Immerhin hat das Bundesverfassungsgericht entschieden, dass jedes Erfassen, Speichern, Abgleichen, Auswerten, Selektieren und Übermitteln von Telekommunikationsdaten einen weiteren Eingriff in Art. 10 GG darstellt.[162] In Betracht kommen allenfalls die Übermittlungsvorschriften des BND-Gesetzes.

Übermittlung nach dem BND-Gesetz

Hinsichtlich der Voraussetzungen für eine Übermittlung an ausländische öffentliche Stellen verweist § 9 Abs. 2 BNDG auf § 19 Abs. 2 und 3 BVerfSchG. Danach darf der BND personenbezogene Daten zum einen an Dienststellen der in Deutschland stationierten Nato-Streitkräfte übermitteln. Zum anderen dürfen solche Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen weitergegeben werden, sofern dies für den BND zur Erfüllung seiner Aufgaben oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist.[163] Soweit allerdings auswärtige Belange der Bundesrepublik oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen, hat eine Übermittlung zu unterbleiben.[164] Unabhängig davon ist eine Übermittlung unter anderem verboten, wenn unter Berücksichtigung der Art der Informationen und ihrer Erhebung die schutzwürdigen Interessen des Betroffenen das Allgemeininteresse an der Übermittlung überwiegen (§ 10 BNDG iVm § 23 Nr. 1 BVerfSchG). Nach dieser Vorschrift ist speziell darauf abzustellen, aus welchem Bereich die Daten stammen und mit welchen Mitteln sie erhoben wurden. Je nach Art und Tiefe des Eingriffs kann somit auch das Recht auf informationelle Selbstbestimmung einer Übermittlung der Daten entgegenstehen.[165] Im Falle einer Übermittlung ist der Empfänger darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden. Außerdem muss der Hinweis erfolgen, dass der BND sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten (§ 9 Abs. 2 BNDG iVm § 19 Abs. 3 S. 4 BVerfSchG). Insgesamt ist der rechtliche Rahmen für Datenübermittlungen an ausländische öffentliche Stellen nach dem BND-Gesetz deutlich weiter als nach dem Artikel 10-Gesetz.

Der Geltungsbereich des BND-Gesetzes, die »Weltraumtheorie« und die »Theorie des virtuellen Auslands«

Die im BND-Gesetz enthaltenen Regelungen über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten (wozu auch die Übermittlungsvorschrift in § 9 zählt) sind gemäß § 1 Abs. 2 S. 2 BNDG nur dann anwendbar, wenn die betreffenden Daten »im Geltungsbereich dieses Gesetzes«, d.h. im Hoheitsgebiet der Bundesrepublik Deutschland erhoben werden.[166] Bei der Überwachung elektronischer Kommunikation lässt sich allerdings darüber streiten, wann es sich im rechtlichen Sinne um eine Datenerhebung im Inland handelt und in welchen Fällen davon auszugehen ist, dass die Daten außerhalb des Bundesgebiets abgeschöpft werden. Der BND folgt bisher etwa der Argumentation, dass die durch Überwachung von Satellitenverbindungen gewonnenen Daten direkt am Satelliten im Weltraum und damit außerhalb des Bundesgebiets erhoben werden (»Weltraumtheorie«).[167] Diese

161 Siehe Huber, »Die strategische Rasterfahndung« [wie Fn. 149], S. 2577, der die Übermittlung personenbezogener Daten aus der Überwachung des Ausland-Ausland-Verkehrs für gänzlich rechtswidrig hält.

162 BVerfGE 100, 313 (359, 366f); 107, 299 (313); 125, 260 (309f).

163 Zum Problem der Feststellung, ob es auf Seiten des Empfängers tatsächlich um die Wahrung erheblicher Sicherheitsinteressen geht, siehe Wolfgang Bock/Otto Mallmann/Wolfgang Roth, »Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG)«, in: Schenke/Graulich/Ruthig (Hg.), *Sicherheitsrecht* [wie Fn. 77], S. 1127–1260 (1242f).

164 Problematisch sind Anfragen von Staaten, die nicht oder nur in unzureichendem Maße über demokratische und rechtsstaatliche Strukturen verfügen. Auswärtige deutsche Belange dürften einer Übermittlung jedenfalls entgegenstehen, wenn absehbar ist, dass die betreffenden Informationen vom Empfänger für Zwecke genutzt werden, die mit den elementaren Menschenrechtsnormen unvereinbar sind. Sofern die Person, auf die sich die erhobenen Daten beziehen, oder ihr nahestehende Personen durch die Übermittlung der Daten dem Risiko einer menschenrechtswidrigen Behandlung (z.B. Folter, rechtswidrige Inhaftierung oder Hinrichtung) ausgesetzt würde, muss die Weitergabe der Informationen ebenfalls unterbleiben, Gusy, »BND-Gesetz« [wie Fn. 91], S. 1298.

165 Bock/Mallmann/Roth, »BVerfSchG« [wie Fn. 163], S. 1252.

166 Gusy, »BND-Gesetz« [wie Fn. 91], S. 1274f, 1300.

167 Siehe die Zusammenfassung der Rechtsauffassung des BND bei Graulich, *Nachrichtendienstliche Fernmeldeaufklärung* [wie Fn. 1], S. 62ff. Siehe auch die Vernehmung der Zeugin Dr. H. F. [wie Fn. 57], S. 10ff. Nach Auffassung des BND stellen Datenerhebungen, die ausschließlich an ausländischen

Argumentation lässt allerdings außer Acht, dass – so die behördliche Datenschutzbeauftragte des BND – »eine deutsche Dienststelle mit Satellitenanlagen, die auf deutschem Boden stehen, die von deutschen Mitarbeitern bedient werden, Daten erhebt«.[168] Zur Erinnerung sei auf die Entscheidung des Bundesverfassungsgerichts von 1999 verwiesen. Darin heißt es, dass durch die Erfassung und Aufzeichnung des Telekommunikationsverkehrs mit Hilfe der auf deutschem Boden stationierten Empfangsanlagen des BND eine technisch-informationelle Beziehung zu den Kommunikationsteilnehmern und ein – den Eigenarten von Daten und Informationen entsprechender – Gebietskontakt hergestellt würden.[169]

Am plausibelsten erscheint es, auf den Standort der technischen Anlagen abzustellen, mittels derer der BND die Telekommunikation überwacht, nicht auf die Quelle der Daten. Bei Informationsoperationen über das Internet wird jedenfalls argumentiert, dass es darauf ankomme, wo der Eintritt ins Netz erfolge.[170] Im Falle der Satellitenüberwachung kann zwischen dem Satelliten als Quelle und der Bodenstation, die die Signale empfängt, unterschieden werden. Befände sich die vom BND genutzte Bodenstation im Ausland, ließe sich dann kaum argumentieren, dass die Datenerhebung tatsächlich im Geltungsbereich des BND-Gesetzes erfolgt. Eine andere Frage ist, wo die Daten verarbeitet und genutzt werden.

Bei der Überwachung von Kabelverbindungen könnte man darauf abstellen, an welchem Punkt die Daten aus dem Kabel in die Erfassungsgeräte und damit in den Herrschaftsbereich des BND übergehen. Danach würden Daten, die an einem Zugriffspunkt in Deutschland erfasst werden, etwa am DE-CIX in Frankfurt am Main, in jedem Fall innerhalb des Geltungsbereichs des BND-Gesetzes erhoben, unabhängig davon, ob die Kabelstrecke das Inland mit dem Ausland verbindet oder ob sie zwischen zwei Punkten im Ausland verläuft und Deutschland nur durchquert. Offenbar wird aber auch die Ansicht vertreten, dass die Erfassung von Daten an Transit-Kabelstrecken in Deutschland so zu behandeln sei wie ein Zugriff auf Kabel außerhalb des Bundesgebiets (»Theorie des virtuellen Auslands«).[171] Die Folge wäre wiederum, dass die datenschutzrechtlichen Regelungen des BND-Gesetzes einschließlich der Übermittlungsvorschrift des § 9 gemäß § 1 Abs. 2 S. 2 BNDG nicht anwendbar wären.

Konsequenzen

Soweit man der »Weltraumtheorie« folgt, wäre die Konsequenz, dass sich die Übermittlung personenbezogener Daten aus satellitengestützter Kommunikation nicht nach § 9 BNDG richtet. Zum selben Ergebnis kommt man nach der »Theorie des virtuellen Auslands«, soweit Daten aus Transit-Kabelverbindungen an Zugriffspunkten in Deutschland erfasst werden. Problematisch ist dieses Ergebnis vor allem deshalb, weil auch die Übermittlungsvorschrift des § 7a G 10 (wie in den vorigen Abschnitten dargelegt) nach Ansicht der Bundesregierung nur für die Weitergabe von Daten gilt, die bei der Überwachung von Deutschland-Ausland-Verkehren (G 10-Verkehre) erhoben werden. Denkbar wäre, dass personenbezogene Daten aus »Routineverkehren«, die über Satelliten laufen, mangels speziellerer Rechtsvorschriften nach dem Bundesdatenschutzgesetz (§ 4b BDSG) an ausländische Nachrichtendienste übermittelt werden dürfen. Das BND-Gesetz schließt die Anwendung dieser und anderer Vorschriften des Bundesdatenschutzgesetzes »[b]ei der Erfüllung der Aufgaben des Bundesnachrichtendienstes« jedoch ausdrücklich aus (§ 11 BNDG).[172] Aus der allgemeinen Aufgabenzuweisung in § 1 Abs. 2 S. 1 BNDG lässt sich auch keine Befugnis zur Übermittlung personenbezogener Daten an ausländische Nachrichtendienste ableiten. Demnach findet die Datenweitergabe in solchen Fällen derzeit offenbar ohne gesetzliche Grundlage statt. Aus den Zeugenvernehmungen vor dem NSA-Untersuchungsausschuss des Bundestages lässt sich entnehmen, dass sich der BND insoweit nur an elementaren Rechtsstaatsprinzipien wie dem Schutz der Menschenwürde, dem Willkürverbot und dem Grundsatz der Verhältnismäßigkeit orientiert.[173]

Lebenssachverhalten ansetzen, generell keine Datenerhebungen im Geltungsbereich des BND-Gesetzes dar.

168 Vernehmung der Zeugin Dr. H. F. [wie Fn. 57], S. 39.

169 BVerfGE 100, 313 (362ff).

170 Gusy, »BND-Gesetz« [wie Fn. 91], S. 1275.

171 Siehe die Diskussion im Rahmen der Vernehmung des Zeugen A. F. [wie Fn. 57], S. 121.

172 Nach § 11 BNDG gilt der Ausschluss für die Erfüllung der Aufgaben des BND generell und nicht nur für die Erhebung personenbezogener Daten im Geltungsbereich des BND-Gesetzes. Nach Aussage der Zeugin Dr. H. F. vor dem NSA-Untersuchungsausschuss [wie Fn. 57], S. 50, vertrete der BND die Position, dass die Überwachung satellitengestützter Kommunikation »insgesamt außerhalb des deutschen Rechtes, damit auch außerhalb des Bundesdatenschutzgesetzes« erfolge.

173 Siehe die Vernehmung der Zeugin Dr. H. F. [wie Fn. 57], S. 11, 29, 72.

Regelungsbedarf

In seiner Kommentierung des BND-Gesetzes spricht der deutsche Verfassungsrechtler Christoph Gusy von einer »Gemengelage aus kaum aufzuklärenden Fakten, regelungsarmen Normen und schwach ausgeprägter gerichtlicher und politischer Kontrolle«. Auf diese Weise entstehe in der Öffentlichkeit der Verdacht von Geheimniskrämerei, nonchalantem Umgang mit gesetzlichen Kompetenzgrenzen und von einem beim BND eher schwach ausgeprägten demokratischen und rechtsstaatlichen Bewusstsein.[174] Unabhängig davon, ob dieser Eindruck in der Öffentlichkeit tatsächlich verbreitet ist, legt die Analyse der aktuellen Gesetzeslage vor dem Hintergrund der verfassungsrechtlichen Anforderungen jedenfalls nahe, dass legislativer Regelungsbedarf besteht. Die Art und Weise, wie der Gesetzgeber die Aufgaben und Befugnisse des BND bislang ausgestaltet hat, mag der Eigenart nachrichtendienstlicher Tätigkeit geschuldet sein und im internationalen Vergleich keine Besonderheit darstellen. Je detaillierter und präziser solche Fragen im Gesetz geregelt sind, desto transparenter wird ein Nachrichtendienst; und je enger seine Befugnisse ausformuliert sind, desto kleiner wird sein Handlungsspielraum.

Dass die Staaten traditionell kein Interesse daran haben, Spionageaktivitäten völkerrechtlich zu regeln oder ihre Dienste nationalen rechtlichen Beschränkungen zu unterwerfen, wurde zu Beginn der Studie bereits ausgeführt (siehe S. 9). Die heutige Überwachung elektronischer Kommunikation besitzt aber eine andere Qualität als die zwischenstaatliche Spionage vergangener Tage. Sie greift nämlich besonders intensiv und in großem Umfang in die Rechte von Privatpersonen ein. Mit dem Rechtsstaatsprinzip, das zu den elementaren Prinzipien des Grundgesetzes zählt, lassen sich unbestimmte oder unklare gesetzliche Regelungen, die zu weitreichenden Grundrechtseingriffen ermächtigen sollen, nicht vereinbaren.[175] Die Anforderungen an die Bestimmtheit und Klarheit von Rechtsnormen sollen nicht nur den Betroffenen in die Lage versetzen, die Rechtslage anhand der gesetzlichen Regelung erkennen zu können; sie dienen auch dazu, die Exekutive zu binden und ihr Verhalten nach Inhalt, Zweck und Ausmaß zu begrenzen; und sie sollen eine effektive gerichtliche Kontrolle ermöglichen.[176] Rechtsvorschriften sind daher grundsätzlich so genau zu fassen, wie dies nach Eigenart der Materie mit Rücksicht auf den Normzweck möglich ist. Je intensiver der Grundrechtseingriff, desto strenger sind die Anforderungen.[177] Besonders weitgehende Bestimmtheitsanforderungen gelten bei heimlichen Überwachungsmaßnahmen.[178] Zudem hat das Bundesverfassungsgericht entschieden, dass – soweit die praktische Bedeutung einer Regelung vom Zusammenspiel der Normen mehrerer Regelungsbereiche abhängt – die Klarheit des Norminhalts und die Voraussehbarkeit der Ergebnisse der Normanwendung gerade auch im Hinblick auf dieses Zusammenwirken gesichert sein müssen.[179]

Es ist nicht ersichtlich, warum das Recht der Nachrichtendienste nicht so umfassend geregelt sein sollte, dass es die gesamte Bandbreite strategischer Kommunikationsüberwachung einschließlich der damit zusammenhängenden Verarbeitung und Nutzung personenbezogener Daten abdeckt. Das berechtigte Interesse an der Geheimhaltung nachrichtendienstlicher Fähigkeiten, Methoden und Verfahren dürfte einer klareren gesetzlichen Aufschlüsselung der Befugnisse jedenfalls kaum entgegenstehen. Auch im Bereich der polizeilichen Gefahrenabwehr und Strafverfolgung sind die Behörden auf operative Geheimhaltung angewiesen, sofern konkrete Überwachungsmaßnahmen durchgeführt werden sollen. Gleichwohl steht außer Frage, dass die dafür notwendigen Befugnisse im Gesetz eindeutig geregelt sein müssen. Jedenfalls dürfen derartige operative Erwägungen nicht dazu führen, dass bereits die Rechtsgrundlagen für solche Aktivitäten »verschleiert« werden. Dabei geht es nicht darum, den politischen, strategischen und taktischen Handlungsspielraum der zuständigen Ministerien und Behörden zu beschneiden (etwa im Hinblick auf die

174 Gusy, »BND-Gesetz« [wie Fn. 91], S. 1265.

175 Zum Bestimmtheitsgebot siehe unter anderem BVerfGE 110, 33 (53ff); Jarass, »Art. 20 GG« [wie Fn. 36], S. 500ff. Kritisch zur mangelnden Bestimmtheit und Klarheit des BND-Gesetzes Gusy, »BND-Gesetz« [wie Fn. 91], S. 1264.

176 BVerfGE 56, 1 (12) – ständige Rechtsprechung.

177 BVerfGE 86, 288 (311); 93, 213 (238).

178 Jarass, »Art. 20 GG« [wie Fn. 36], S. 502.

179 BVerfGE 108, 52 (Rn. 56); 110, 33 (53f).

Fokussierung auf bestimmte Gefahrenbereiche und Konfliktregionen oder auf die Auswahl bestimmter Überwachungsziele).

Wie aus Presseberichten hervorgeht, arbeitet die Bundesregierung bereits an einer Reform der gesetzlichen Rahmenbedingungen, unter denen der BND aktiv werden darf und unter denen er kontrolliert wird.[180] Im Zuge eines solchen Vorhabens sollten unter anderem die folgenden Punkte berücksichtigt werden:

- *Regelung der strategischen Überwachung von Ausland-Ausland-Kommunikation und des Umgangs mit »Routineverkehren«.* Gerade die strategische Überwachung von Kommunikationsverkehren, bei denen sich beide Teilnehmer im Ausland befinden (»Routineverkehre«), ist für den BND, dessen Aufgabe darin besteht, Erkenntnisse über das Ausland zu gewinnen, von besonderem Interesse. Rechtlich unzureichend abgesichert ist derzeit nicht nur die Überwachung und Aufzeichnung solcher Verkehre, sondern auch die Übermittlung personenbezogener Daten an ausländische Nachrichtendienste, soweit es sich um Daten handelt, die durch die Überwachung von Ausland-Ausland-Kommunikation gewonnen werden. Die Regelungsdefizite in diesem Bereich wurden auf S. 32 und S. 34ff ausführlich beschrieben.
- *Regelung der Erhebung personenbezogener Daten außerhalb des Geltungsbereichs des BND-Gesetzes (jenseits der strategischen Fernmeldeaufklärung) und der sich daran anschließenden Verarbeitung und Nutzung der Daten.* Dieser Fall wäre beispielsweise relevant, wenn der BND im Rahmen einer Kooperation Zugang zu Einrichtungen im Ausland hätte, um personenbezogene Daten zu erheben. Die extraterritoriale Dimension nachrichtendienstlicher Informationsgewinnung wird im BND-Gesetz nahezu vollständig ausgeblendet (siehe dazu die Ausführungen auf S. 35f).[181] Daher ist zum Beispiel nicht ersichtlich, auf welcher Grundlage im Ausland erhobene personenbezogene Daten an ausländische Nachrichtendienste übermittelt werden dürfen.
- *Regelung des Umgangs mit personenbezogenen Daten, die dem BND von ausländischen Nachrichtendiensten übermittelt werden.* Auch in dieser Hinsicht besteht Klärungsbedarf. Fraglich ist etwa, ob es sich bei der Entgegennahme der Daten um ein Erheben im Geltungsbereich des BND-Gesetzes handelt. Dann wäre das BND-Gesetz auf die Verarbeitung und Nutzung der Daten anwendbar. Andernfalls bedürfte es einer gesonderten gesetzlichen Grundlage.[182] Ausländer sind durch das Recht auf informationelle Selbstbestimmung gegenüber der deutschen öffentlichen Gewalt in gleicher Weise wie deutsche Staatsangehörige geschützt, soweit ihre personenbezogenen Daten in Deutschland verarbeitet oder genutzt werden.
- *Ausweitung der parlamentarischen Kontrolle.* Auf S. 31f wurde die Funktion des Parlamentarischen Kontrollgremiums und der G 10-Kommission beschrieben. Eine detaillierte Analyse der strukturellen Defizite und sonstigen Schwächen der bestehenden Mechanismen ist nicht Gegenstand dieser Studie.[183] Generell besteht aber Konsens darüber, dass diese Mechanismen reformiert werden müssen, um eine effektivere Kontrolle der strategischen Überwachung elektronischer Kommunikation zu gewähr-

180 Siehe z.B. »Entwurf für ein neues BND-Gesetz: Eine Art No-Spy-Klausel für Europa?«, *tagesschau.de*, 18.1.2016, <https://www.tagesschau.de/inland/bnd-reform-103.html>; Michael Götschenberg, »Konsequenzen der BND-Ausspähaffäre: Personalwechsel elegant begründet«, *tagesschau.de*, 17.12.2015, <https://www.tagesschau.de/inland/bnd-281.html>; Manuel Bewarder, »Wen darf der BND überwachen? Auslegungssache«, *welt.de*, 17.5.2015, <www.welt.de/141043665>. Siehe dazu auch das Eckpunktepapier der SPD-Bundestagsfraktion »Rechtsstaat wahren – Sicherheit gewährleisten! Erste Konsequenzen aus dem NSA-Skandal: Eckpunkte der SPD-Bundestagsfraktion für eine grundlegende Reform der Strategischen Fernmeldeaufklärung des BND mit internationaler Vorbildwirkung«, 16.6.2015, <www.spdfraktion.de/sites/default/files/2015-06-16-eckpunkte_reform_strafma-r-endfassung.pdf> (Zugriff jeweils am 12.4.2016).

181 Einzige Ausnahme ist die allgemeine Aufgabenzuweisung in § 1 Abs. 2 S. 1 BNDG, unter die sich die Sammlung von Informationen im Ausland und deren Auswertung nämlich problemlos subsumieren lässt. Zwar kann der deutsche Gesetzgeber etwa Auskunftspflichten von Unternehmen gegenüber dem BND nur insoweit regeln, wie die betreffenden Unternehmen deutscher Hoheitsgewalt unterliegen. Selbstverständlich können aber die Voraussetzungen, unter denen Organe der deutschen öffentlichen Gewalt zu extraterritorialem Handeln nach deutschem Recht befugt sein sollen, gesetzlich fixiert werden, Bäcker, *Stellungnahme zur Anhörung* [wie Fn. 80], S. 22. Außerdem fehlt es im BND-Gesetz an konkreten Vorgaben für die Verarbeitung und Nutzung im Ausland erhobener personenbezogener Daten.

182 Siehe dazu Papier, *Gutachterliche Stellungnahme* [wie Fn. 83], S. 8.

183 Siehe dazu z.B. die weitreichenden Vorschläge von Löning, *Reformagenda* [wie Fn. 109], S. 5ff; siehe auch Stefan Heumann/Thorsten Wetzling, *Strategische Auslandsüberwachung: Technische Möglichkeiten, rechtlicher Rahmen und parlamentarische Kontrolle*, Berlin: Stiftung Neue Verantwortung, Mai 2014 (Policy Brief), S. 16ff.

leisten. Dies betrifft insbesondere auch die Überwachung von Ausland-Ausland-Kommunikation. Derzeit erstreckt sich etwa die Kontrolle durch die G 10-Kommission nur auf die Überwachung von Kommunikationsverkehren zwischen Deutschland und dem Ausland.

Das übergeordnete Ziel einer solchen Reform sollte sein, den BND auf rechtlich sicherem Boden zu stärken. Gleichzeitig geht es darum, auf der internationalen Bühne weiterhin als glaubwürdiger Verfechter der Menschenrechte und der »Rule of Law« aufzutreten. Die notwendige Kritik an der anlasslosen, globalen und massenhaften Kommunikationsüberwachung, wie sie von den Nachrichtendiensten anderer Staaten betrieben wird, lässt sich nur dann seriös formulieren, wenn die eigene Praxis rechtsstaatlichen Standards entspricht.

Lektüre-Empfehlungen

Marcel Dickow
Außenpolitik der Dienste. Die Strategische Kommunikationsüberwachung und ihre Folgen
SWP-Aktuell 18/2015, Februar 2015, <https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2015A18_dkw.pdf>

Annegret Bendiek
Umstrittene Partnerschaft. Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit
SWP-Studie 26/2013, Dezember 2013, <https://www.swp-berlin.org/fileadmin/contents/products/studien/2013_S26_bdk.pdf>

Abkürzungsverzeichnis

Abs./S./Nr./lit.	Absatz/Satz/Nummer/Buchstabe
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BR-Drs.	Drucksache des Bundesrates
BT-Drs.	Drucksache des Deutschen Bundestages
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz)
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
COMINT	Communication Intelligence
EMRK	Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten
EU	Europäische Union
GCHQ	Government Communications Headquarters
G 10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz)
GG	Grundgesetz für die Bundesrepublik Deutschland
IP	Internet Protocol
iVm	in Verbindung mit
mwN	mit weiteren Nachweisen
Nato	North Atlantic Treaty Organization
NSA	National Security Agency
PKGrG	Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz)
Rn.	Randnummer
SIGINT	Signals Intelligence
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
TKÜV	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung)
UN	United Nations
URL	Uniform Resource Locator