

## Unterrichtung

durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

### Abhöraktivitäten US-amerikanischer Nachrichtendienste in Deutschland

Bericht an den Deutschen Bundestag gemäß § 26 Absatz 2 des Bundesdatenschutzgesetzes

#### A. Einleitung

Die jüngsten Erkenntnisse zur Überwachung der Kommunikation durch ausländische Nachrichtendienste verdeutlichen die Dimension der massenhaften heimlichen und weitgehend anlasslosen Erhebung, Speicherung und Verarbeitung elektronischer Daten. Neben den Überwachungsaktivitäten ausländischer Nachrichtendienste (AND) ist dabei auch die Arbeit deutscher Nachrichtendienste (ND) und deren Zusammenarbeit mit ausländischen Partnern in den Blick zu nehmen.

Das vorliegende Papier soll ein Diskussionsbeitrag sein und dem Bundestag Anhaltspunkte für mögliche Entscheidungen und Weichenstellungen geben.

#### B. Kernaussagen

- Grundrechtsschutz und Sicherheit müssen insbesondere im Bereich der Nachrichtendienste in einem ausgewogenen Verhältnis stehen. Dies setzt eine effektive und lückenlose unabhängige Kontrolle nachrichtendienstlicher Tätigkeiten voraus.
- Die berichteten anlasslosen Massendatenerhebungen sind schnell, umfassend, detailliert und – soweit rechtlich zulässig – auch öffentlich aufzuklären.
- Strukturelle und/oder regelungstechnische Defizite sind unverzüglich und nachhaltig zu beseitigen – auf nationaler wie internationaler Ebene.
- Die Zusammenarbeit deutscher mit ausländischen Nachrichtendiensten darf nicht dazu führen, durch Aufgabenteilung nationale (verfassungs-)rechtliche Beschränkungen für ihre Tätigkeit zu umgehen („Befugnis-Hopping“).
- Aufgrund der Gesetzgebungs- und Kontrollkompetenz des Deutschen Bundestages über die Nachrichtendienste des Bundes ist eine engere Kooperation der parlamentarisch bestellten Kontrollorgane und die Beseitigung bestehender Kontrolldefizite dringend erforderlich.

#### C. Sachstand

##### Ausgangspunkt: Enthüllungen zu anlasslosen Massendatenerhebungen

Nach den Medienberichten über die Enthüllungen von Edward Snowden haben US-amerikanische und britische Nachrichtendienste anlasslos massenhaft Telekommunikationsverkehre (Telefonate, E-Mails, SMS etc.) überwacht, gespeichert und analysiert – in einem bis dato unvorstellbaren Ausmaß. Nicht deutlich ist dabei bis heute, inwieweit auch Daten auf deutschem Territorium durch AND überwacht werden. Als gesichert kann aber

gelten, dass auch deutsche Kommunikationsteilnehmer und Internetnutzer von anlasslosen Massendatenerhebungen betroffen sind. Daneben werden offenbar gezielt einzelne Zielpersonen ausgeforscht, auch Politikerinnen und Politiker in höchsten Staatsämtern. Mit dem Kampf gegen den Terror und gegen die Verbreitung von Massenvernichtungswaffen – wie von US-Seite immer wieder zur Begründung angeführt – können derartige Maßnahmen nicht gerechtfertigt werden.

Diese Vorgänge müssen zeitnah, umfassend und detailliert aufgeklärt werden. Dabei geht es nicht nur darum, Gesetzesverstöße aufzudecken. Vielmehr sind ebenso (strukturelle) Fehler und Defizite im deutschen, europäischen und internationalen Recht zu ermitteln und zu beseitigen, auch und insbesondere bei der Tätigkeit von Nachrichtendiensten. Dabei sind sowohl die Tätigkeit der deutschen Nachrichtendienste und ihre Kooperation mit ausländischen Partnern als auch die Tätigkeit der AND in Deutschland in den Blick zu nehmen.

Die Bundeskanzlerin hat zutreffend betont, dass auch die ausländischen Nachrichtendienste bei ihren Aktivitäten in Deutschland das deutsche Recht beachten müssen. Bei der Rechtsdurchsetzung bestehen aus meiner Sicht aber erhebliche Defizite. Deshalb halte ich die Optimierung der parlamentarischen und datenschutzrechtlichen Kontrollinstrumente für geboten.

Der Deutsche Bundestag und die Landesparlamente bestimmen als Vertretungsorgane der Bürgerinnen und Bürger über die gesetzlichen Vorgaben, die auch von den Nachrichtendiensten zu beachten sind. Zugleich kontrollieren die Parlamente bzw. die von ihnen beauftragten Organe, ob diese Vorgaben beachtet werden. Nachrichtendienste dürfen kein „Staat im Staate“ sein oder ein „Eigenleben“ führen. Sie sind Teil der Exekutive. Damit unterstehen sie uneingeschränkt der Entscheidungsgewalt der Legislative. Die Macht geht damit vom Volk und nicht den Nachrichtendiensten aus. Auch die Datenschutzbeauftragten des Bundes und der Länder sind gesetzlich zur Kontrolle der Einhaltung einschlägiger datenschutzrechtlicher Vorgaben verpflichtet. Um diese Aufgaben wahrzunehmen, sind sie auf die Unterstützung der Nachrichtendienste und der für die Dienst- und Fachaufsicht zuständigen Ministerien angewiesen. Hier haben sich insbesondere hinsichtlich der Aufklärung der auf die Snowden-Papiere zurückgehenden Sachverhalte erhebliche Schwierigkeiten ergeben, die mich zu einer förmlichen Beanstandung gemäß § 25 BDSG veranlasst haben.

### **Sind Nachrichtendienste an Grundrechte gebunden?**

Staatliche Stellen sind in ihrem Handeln an Recht und Gesetz gebunden. Die Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht (Art. 1 Abs. 3 Grundgesetz (GG)). Dies gilt im hier diskutierten Zusammenhang speziell für das Post- und Fernmeldegeheimnis (Art. 10 GG). Auch der Datenschutz hat – entsprechend der ständigen Rechtsprechung des Bundesverfassungsgerichts – Grundrechtsrang: Das „Grundrecht auf informationelle Selbstbestimmung“ soll es dem Einzelnen ermöglichen, grundsätzlich selbst über die Preisgabe und Verwendung der ihn betreffenden Daten zu entscheiden. Besonderen verfassungsrechtlichen Schutz genießt der unantastbare Kernbereich privater Lebensgestaltung, der bei jeglicher staatlicher Tätigkeit zu beachten ist. Zudem hat das Bundesverfassungsgericht ein Grundrecht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ festgestellt.

Grundrechtseingriffe erfolgen grundsätzlich offen und unterliegen der gerichtlichen Überprüfung (Art. 19 Abs. 4 GG). Aus diesem Grund bedarf die Tätigkeit von Nachrichtendiensten, die im Allgemeinen heimlich agieren, einer besonderen Rechtfertigung. Da den Betroffenen hinsichtlich der durch diese Tätigkeit verursachten Grundrechtseingriffe der Rechtsweg – falls überhaupt – nur sehr eingeschränkt zur Verfügung steht, sind zudem besondere Schutzvorkehrungen erforderlich, sowohl hinsichtlich der Tätigkeit der ND selbst als auch im Hinblick auf deren Kontrolle.

Entsprechend dem dem Grundgesetz zugrunde liegenden Konzept der „wehrhaften Demokratie“ haben sich die Gesetzgeber von Bund und Ländern für die Einrichtung von Nachrichtendiensten entschieden. Zur Erfüllung ihrer Aufgaben können deutsche Nachrichtendienste auch auf Hinweise zurückgreifen, die sie z. B. aufgrund von Kooperationsvereinbarungen von AND erhalten. Auch in dieser Hinsicht unterliegen die ND jedoch der Grundrechtsbindung. Ihnen ist die Umgehung der durch das Grundgesetz vorgegebenen Grundrechte durch Kooperationsbeziehungen zu AND ebenso untersagt wie bei der eigenen nachrichtendienstlichen Tätigkeit.

Bestehen tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen, dürfen deutsche Nachrichtendienste bezogen auf den jeweiligen Aufgabenbereich Personen und Strukturen, von denen Gefährdungen ausgehen – auch heimlich, d. h. unbemerkt – überwachen und in diesem Zusammenhang erforderliche Daten erheben und auswerten. Damit können sie – anders als die Polizei – bereits tätig werden, bevor eine konkrete Gefahr von diesen Personen oder Organisationen ausgeht. Sie haben jedoch keine exekutiven Befugnisse, d. h. sie dürfen z. B. niemanden durchsuchen, vernehmen oder festnehmen. Dies darf nur die Polizei.

Vor dem Hintergrund der geschichtlichen Erfahrungen mit der Geheimen Staatspolizei („Gestapo“) im Nationalsozialismus hat der Verfassungs- und Gesetzgeber Polizeien und Nachrichtendiensten bewusst unterschiedliche Aufgaben und Befugnisse zugewiesen. Die klare Trennung dieser Behörden muss auch bei deren informativ-er Zusammenarbeit beachtet werden. Das hat das Bundesverfassungsgericht in seiner aktuellen Entscheidung zum Antiterrordateigesetz nachdrücklich betont.

### **Spannungsverhältnis – Heimlichkeit und Grundrechtsschutz**

Aufgrund der heimlichen Tätigkeit der Nachrichtendienste merken Betroffene regelmäßig nicht, wenn sie beobachtet und überwacht werden. Sie werden hierüber in aller Regel auch nicht informiert. Auch die verfassungsrechtlich gebotene nachträgliche Benachrichtigung unterbleibt vielfach, wie datenschutzrechtliche Kontrollen wiederholt ergeben haben. Wer nicht weiß, dass er beobachtet wird, kann dies auch nicht (gerichtlich) überprüfen lassen. Im Bereich der Nachrichtendienste besteht daher ein besonderes Spannungsverhältnis zwischen dem Schutz der Grundrechte der Betroffenen und dem Auftrag des Staates, Sicherheit zu gewährleisten. Folglich ist die Kontrolle der Nachrichtendienste von besonderer Bedeutung. Hierfür müssen angemessene und effiziente Kontroll- und Überprüfungsmechanismen zur Verfügung stehen.

Demgegenüber ist die Tätigkeit der Polizei für einen Betroffenen regelmäßig erkenn- und (gerichtlich) überprüfbar. Es existieren gesetzlich festgelegte, transparente und öffentliche Verfahren. Diese gewähren den Betroffenen weitreichende Rechte.

### **Welche Nachrichtendienste gibt es in Deutschland und auf welcher Rechtsgrundlage arbeiten sie?**

Deutsche Nachrichtendienste sind

- das Bundesamt für Verfassungsschutz (BfV) (zuständig für das Inland),
- der Bundesnachrichtendienst (BND) (zuständig für das Ausland),
- der Militärische Abschirmdienst (MAD) (zuständig für die Bundeswehr) und
- die Landesämter für Verfassungsschutz (LfV) (zuständig für das jeweilige Bundesland).

Für jeden dieser Dienste gelten gesonderte Rechtsgrundlagen, die er beachten muss:

- BfV: „Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz“ (BVerfSchG).
- BND: „Gesetz über den Bundesnachrichtendienst“ (BND-G).
- MAD: „Gesetz über den militärischen Abschirmdienst“ (MAD-G).
- LfV: Spezielle Landesgesetze.

Das BND-G und das MAD-G verweisen vielfach auf das BVerfSchG.

Nach dem BVerfSchG, BND-G und MAD-G sind auch Vorgaben des Bundesdatenschutzgesetzes (BDSG) zu beachten.

### **Wie wird das besonders bedeutsame Brief-, Post- und Fernmeldegeheimnis angesichts nachrichtendienstlicher Tätigkeit geschützt?**

Artikel 10 GG (Brief-, Post und Fernmeldegeheimnis) schützt sowohl die Inhalte als auch die Verkehrsdaten („Metadaten“) der Kommunikation. Eingriffe der Nachrichtendienste in das Grundrecht aus Artikel 10 GG sind besonders schwerwiegend. Daher existiert hierfür eine besondere Rechtsgrundlage – das „Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses“ (G 10).

Das G 10 gestattet BfV, BND und MAD, die Telekommunikationsverkehre eines Betroffenen (z. B. seine Telefonate sowie seine Kommunikation im Internet) zu überwachen. Die Voraussetzungen hierfür sind bewusst eng gefasst.

Wegen fehlender deutscher Eingriffsermächtigungen sind entsprechende Überwachungsmaßnahmen ausländischer Dienste, bei denen Verkehrsdaten oder Inhalte der Kommunikation erhoben, verarbeitet oder genutzt werden, nach deutschem Recht unzulässig.

**Wie gefährden die strategische Fernmeldeüberwachung und die Zusammenarbeit mit AND die im deutschen Recht implementierten Schutzmechanismen?**

Das G 10 gewährt dem BND eine weitere, besondere, Befugnis. Er darf sog. „internationale Telekommunikationsbeziehungen“, d. h. Telekommunikationsverkehre, die über einen bestimmten technischen Knotenpunkt (Server) von Deutschland aus ins Ausland (in bestimmte Staaten/Gebiete) oder von dort aus nach Deutschland erfolgen, automatisiert erfassen, speichern und auswerten (sog. strategische Fernmeldeüberwachung (SFÜ)).

Im Vergleich zur Überwachung eines Betroffenen ist die SFÜ eine Massendatenerhebung. So darf der BND bis zu zwanzig Prozent aller über den jeweiligen Knotenpunkt abgewickelten Telekommunikationsverkehre nach vordefinierten Suchbegriffen durchsuchen (rastern). Alle Treffer werden vom BND ausgeleitet, gespeichert und analysiert. Die entsprechenden Daten können – nach den Vorgaben des G 10 – auch an ausländische Stellen, z. B. AND, übermittelt werden.

Eine technisch bedingt zwangsläufige Folge der SFÜ ist, dass auch Telekommunikationsverkehre von unbescholtenen Bürgern betroffen sind. Denn aufgrund des technischen Fortschritts werden Telekommunikationsverkehre heute in aller Regel digital über das Internet (d. h. über Server) geleitet. Infolgedessen ist die Anzahl der an den Knotenpunkten erfassten Daten massiv angewachsen und damit auch die Zahl der (potentiell) betroffenen unbeteiligten Personen.

Nach dem G 10 darf der BND mit der SFÜ keine inländischen Telekommunikationsverkehre erfassen, d. h. keine zwischen Personen in Deutschland geführte Kommunikation. Aufgrund der Digitalisierung der Telekommunikationsverkehre können diese inländischen Verkehre allerdings ebenfalls von deutschen Knotenpunkten über ausländische Server zum Empfänger nach Deutschland geleitet werden (siehe auch meinen 24. Tätigkeitsbericht, Nr. 7.7.4 – [www.bfdi.bund.de](http://www.bfdi.bund.de)).

Für die Betroffenen ist der jeweilige Übertragungsweg nicht erkennbar. Er wird systemisch und automatisiert gewählt, abhängig z. B. von der Kapazitätsauslastung, der Verfügbarkeit bestimmter Übertragungsrouten oder Kostengesichtspunkten. So kann ein in Deutschland geführtes Telefonat über den „Umweg“ eines Servers in den USA und/oder anderen Staaten geleitet werden.

Die AND in diesen ausländischen Staaten sind – oftmals in Übereinstimmung mit dem dort geltenden Recht – in der Lage, diese Telekommunikationsverkehre zu erfassen und für ihre Zwecke zu nutzen. Damit wird die Schutzfunktion des zumindest für innerdeutsche Telekommunikationsverkehre geltenden – und auch auf die umgeleiteten Telekommunikationsverkehre grundsätzlich anwendbaren – Telekommunikationsgeheimnisses durchbrochen.

Grundrechtsrelevant sind derartige Praktiken insbesondere, sofern diese Daten von einem AND unaufgefordert oder aufgrund bestehender Kooperationsvereinbarungen an deutsche Nachrichtendienste übermittelt und von letzteren verwendet werden, obgleich sie die Daten nach deutschem Recht nicht hätten erheben dürfen. Damit können nationale (verfassungs-)rechtliche Beschränkungen (z. B. der vom Bundesverfassungsgericht geforderte absolute Schutz des Kernbereichs der privaten Lebensgestaltung) unterlaufen bzw. umgangen werden.

Diese Problematik besteht auch, wenn die Daten von einem AND illegal in Deutschland erhoben und an einen deutschen ND übermittelt worden sind. In diesem Fall begeht der AND nach deutschem Recht eine Straftat – ebenso verhält sich der empfangende deutsche Nachrichtendienst rechtswidrig, sofern dieser von der illegalen Datenerhebung Kenntnis hat.

Diese Problematik könnte ggf. durch den Abschluss internationaler Abkommen über die Tätigkeit der Nachrichtendienste im jeweiligen In- und Ausland entschärft werden, die rechtliche und technische Mindeststandards für die nachrichtendienstlichen Aktivitäten gewährleisten.

**Kontrolle der deutschen Nachrichtendienste – umfassend und effizient?**

Die wirksame und effiziente Kontrolle der Nachrichtendienste ist von herausragender Bedeutung.

In Deutschland üben der Deutsche Bundestag bzw. die Länderparlamente diese Kontrolle mit Hilfe der von ihnen bestellten Kontrollorgane aus. Auf Bundesebene sind dies

- das aus Mitgliedern des Deutschen Bundestages bestehende Parlamentarische Kontrollgremium (PKGr),
- die vom PKGr bestellte G 10-Kommission, deren Mitglieder nicht dem Deutschen Bundestag angehören müssen und
- der vom Deutschen Bundestag gewählte Beauftragte für den Datenschutz und die Informationsfreiheit (BfDI).

Die Kontrollorgane haben (teilweise) unterschiedliche Aufgaben und Befugnisse.

Das PKGr kontrolliert die Tätigkeit der Nachrichtendienste des Bundes, d. h. umfassend auch in fachlicher Hinsicht sowie in Bereichen, in denen keine personenbezogenen Daten verarbeitet werden. Rechtsgrundlage hierfür ist das Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG).

Soweit die Nachrichtendienste personenbezogene Daten erheben oder verarbeiten, ist auch der BfDI kontrollbefugt – jedoch nicht für personenbezogene Daten, die nach dem G 10 erhoben worden sind. Diese kontrolliert ausschließlich die G 10-Kommission.

Als vom Deutschen Bundestag bestelltes Kontrollorgan hat der BfDI auf Anforderung des Parlaments nicht nur Gutachten zu erstellen und Berichte zu erstatten, sondern auch Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei öffentlichen Stellen des Bundes nachzugehen (vgl. § 26 Absatz 2 BDSG).

Damit das Parlament seine Gesetzgebungs- und Kontrollkompetenz über die Nachrichtendienste bestmöglich ausüben kann, müssen alle Kontrollorgane enger kooperieren. Zudem müssen sie sowohl rechtlich wie auch tatsächlich in der Lage sein, ihre Aufgaben effizient und angemessen zu erfüllen. Dies ist derzeit nicht der Fall. Es bestehen gravierende Defizite, die u. a. zu kontrollfreien Räumen führen (siehe u. a. meinen 24. Tätigkeitsbericht, Punkt 7.7.1 ff – [www.bfdi.bund.de](http://www.bfdi.bund.de)). Damit ist das System der „Checks and Balances“ in eine Schiefelage geraten, die dringend korrigiert werden muss.

Auf EU-Ebene gibt es mangels Zuständigkeit für nachrichtendienstliche Fragen eine harmonisierte datenschutzrechtliche Kontrollstruktur im Hinblick auf die nationalen Nachrichtendienste weder nach geltendem noch nach den zur Zeit in Brüssel verhandelten neuen datenschutzrechtlichen Instrumentarien. Sowohl die im Entwurf vorliegende Datenschutz-Grundverordnung als auch die zugehörige Richtlinie gelten in diesem Zusammenhang nur für beteiligte Telekommunikationsunternehmen, die das Fernmeldegeheimnis gewährleisten müssen. Die Überwachung durch Drittstaaten wird allerdings bei der Frage relevant, inwieweit der drittstaatliche Zugriff auf bei Telekommunikationsanbietern gespeicherte Daten von Unionsbürgern davon abhängig gemacht wird, ob mitgliedstaatliche Datenschutzbehörden eine Genehmigung hierzu erteilen oder der Zugriff zumindest ihnen und ggf. den Betroffenen gegenüber meldepflichtig ist.

### **Scheitert die Wirksamkeit von Kontrollbefugnissen an der technischen Wirklichkeit?**

Zu den angesprochenen Kontrolllücken, die sich aus der Struktur der Kontrollbefugnisse ergeben, stellt sich noch die Frage, wie die bestehenden, vom Bundestag abgeleiteten Kontrollbefugnisse praktisch-technisch umgesetzt werden können. Sind die theoretischen Vorgaben faktisch umfänglich und effizient umsetzbar? Dies ist zumindest zweifelhaft. Denn einerseits werden – wie gezeigt – teilweise auch rein inländische Telekommunikationsverkehre über das Ausland geleitet. Dadurch verliert das Telekommunikationsgeheimnis nicht seine Geltung. Fraglich ist aber, wie es angesichts dessen noch durchsetzbar ist.

Hinzu kommen die sehr weitreichenden technischen Möglichkeiten von AND, auch außerhalb der Zusammenarbeit mit deutschen Diensten Massendatenerfassungen zu betreiben. Die Öffentlichkeit und die zur Kontrolle der Nachrichtendienste berufenen Organe sehen sich mithin mit einer höchst unübersichtlichen Gemengelage konfrontiert. Diese resultiert aus der Vielzahl in- und ausländischer Akteure, vielgestaltigen Datenströmen, unterschiedlichen Rechtsregimen und den damit verbundenen rechtlichen Kollisionen. Aus dieser Gemengelage ergeben sich mannigfaltige Spannungslagen, die allerdings keinesfalls als Argument dafür herhalten dürfen, die praktische Wirksamkeit der Befugnisse der Kontrollorgane zu schmälern.

### **Dürfen ausländische Dienste deutsche Telekommunikation überwachen?**

Die Tätigkeit von Nachrichtendiensten richtet sich zunächst nach dem jeweiligen nationalen Recht. Völkerrechtlich ist Spionage für sich genommen zumindest nicht verboten, was vor allem aus ihrer verbreiteten und gängigen Praxis hergeleitet wird. Soweit AND allerdings in Deutschland tätig werden, ist dies nach deutschem Recht zu beurteilen. Dies bedeutet, dass Eingriffe von AND in deutsche Grundrechte nach deutschem Recht unzulässig sind, jedenfalls dann, wenn sie auf deutschem Boden erfolgen. Maßnahmen von AND können auch dann strafbar sein, wenn sie zwar im Ausland erfolgen, sich aber als Straftaten in Deutschland verwirklichen. Dies kann z. B. bei Eingriffen in das Post- und Fernmeldegeheimnis oder bei Zugriffen auf IT-Systeme aus dem Ausland der Fall sein.

In diesem Zusammenhang ist auch über die Besonderheiten diskutiert worden, die sich aus dem ehemaligen Besatzungsstatus Deutschlands ergeben. Nach meiner Kenntnis gibt es für ausländische Dienste – auch für AND der NATO-Staaten – keine Rechtsgrundlage für deren Tätigwerden gegenüber deutschen Grundrechtsträgern

aus Abkommen, die den Aufenthalt der NATO-Streitkräfte auf deutschem Boden regeln. Im Gegenteil: Auch Liegenschaften, die durch ausländische Truppenverbände genutzt werden, bleiben Teil des deutschen Staatsgebietes und es gilt deutsches Recht. NATO-Streitkräfte haben dieses zu achten. Gleichwohl ist nicht auszuschließen, dass von solchen Liegenschaften aus deutsche Telekommunikationsverkehre ins Visier genommen werden, die Truppenverbände also außerhalb ihres Bündisauftrags tätig werden.

Allerdings sind Handlungsmöglichkeiten deutscher Behörden in Bezug auf solche Liegenschaften äußerst begrenzt. Dies gilt auch für die Datenschutzkontrolle. So habe ich – wie die Datenschutzbeauftragten der Länder – keine datenschutzrechtlichen Kontrollbefugnisse in Bezug auf diese Liegenschaften und hinsichtlich der Tätigkeit der dort tätigen ausländischen Stellen.

Die einschlägigen Abkommen sind von dem Gedanken der Zusammenarbeit geleitet und von Verfahrensregelungen geprägt, die auf die weitgehend konsensuale Beilegung aufkommender Streitigkeiten oder Mißstimmigkeiten ausgerichtet sind. Zwar ist etwa im Zusatzabkommen zum NATO-Truppenstatut hinsichtlich der in Deutschland stationierten ausländischen Truppen ein Streitbeilegungsmechanismus vorgesehen, im Rahmen dessen auch die Frage nach unerlaubten Überwachungstätigkeiten von NATO-Liegenschaften aus thematisiert werden könnte. Allerdings sind die in diesem Verfahren gefundenen Lösungen letztlich nicht durchsetzbar. Hinzu kommt, dass die Initiative zur Nutzung solcher Mechanismen vom politischen Willen der Bundesregierung abhängig ist.

Noch schwieriger stellt sich die Lage dar, wenn nachrichtendienstliche Tätigkeiten – etwa die Überwachung von Regierungskreisen des Gastlandes – von diplomatischen oder konsularischen Vertretungen aus erfolgen. In solchen Fällen ist aufgrund des besonderen Schutzes solcher Vertretungen die Sach- und Rechtsaufklärung praktisch unmöglich.

### **Lässt sich die Überwachung auf internationaler Ebene verhindern?**

Das zentrale rechtliche Problem internationaler nachrichtendienstlicher Überwachungsaktivitäten besteht in der territorialen Begrenztheit rechtlicher Vorgaben und der Möglichkeiten zu ihrer Durchsetzung bei zunehmender Globalisierung der Datenverarbeitung. Die Lösung dieser Problematik kann prinzipiell auf zwei Ebenen erfolgen: durch Gewährleistung internationaler rechtlicher Standards, die – ungeachtet des physischen Orts der Datenverarbeitung – gleichermaßen für eigene und fremde Staatsbürger gelten oder durch technische Maßnahmen, die die Zugriffsmöglichkeiten von AND auf deutsche bzw. europäische Daten minimieren.

### **Welche europäischen oder internationalen Rechtsinstrumente können die Überwachung begrenzen?**

Die Aktivitäten der Bundesregierung zur Verhinderung des Zugriffs insbesondere US-amerikanischer Nachrichtendienste auf innerdeutsche Telekommunikationsverkehre sind zu begrüßen. Ob ein in diesem Zusammenhang diskutiertes „No Spy-Abkommen“ überhaupt zu Stande kommt, erscheint derzeit zweifelhaft. Unzureichend wäre es auch, wenn es sich hierbei lediglich um ein (Geheim-)Abkommen zwischen Geheimdiensten handeln würde, das gegenüber deutschen Grundrechtsträgern keine justiziable Schutzwirkung entfaltet.

Zudem wäre von einem solchen Abkommen nicht zu erwarten, dass es die massenweise Erhebung und Verarbeitung von Daten deutscher Bürgerinnen und Bürger durch AND begrenzen könnte, soweit auf die Daten außerhalb des deutschen Territoriums zugegriffen wird.

Abgesehen von diesem bilateralen Ansatz wird sich die Generalversammlung der Vereinten Nationen in den kommenden Wochen mit einem von Brasilien und Deutschland eingebrachten Resolutionsentwurf befassen, der auf die massenhafte und weitgehend anlasslose Überwachung des Telekommunikationsverkehrs und das gezielte Ausspähen von Regierungen und Unternehmen reagiert. Die Resolution „The Right to Privacy in the Digital Age“ hat die Fortentwicklung der internationalen Bemühungen zum effektiveren Schutz der Privatsphäre zum Ziel. Auch wenn sie nach derzeitigem Stand gute Chancen auf eine breite Mehrheit in der Generalversammlung hat, ist sie völkerrechtlich nicht bindend.

Im Zusammenhang mit der EU-Datenschutz-Grundverordnung wird ein Vorschlag diskutiert, der den Zugriff von Behörden aus Drittstaaten auf Daten, die dem europäischen Datenschutzrecht unterliegen, von der Genehmigung der jeweils zuständigen Datenschutzbehörden der Mitgliedstaaten abhängig macht. Sowohl die Bundesregierung als auch der Innen- und Rechtsausschuss des Europäischen Parlaments haben sich für eine derartige Regelung ausgesprochen. Diese Regelung würde auch auf entsprechende Aktivitäten der US-amerikanischen National Security Agency (NSA) anwendbar sein, etwa im Hinblick auf Daten europäischer Provenienz, die in Cloud-Services gespeichert werden. Allerdings ist zweifelhaft, inwieweit US-Behörden und in den USA ansässige Unternehmen bereit sind, sich an entsprechende Vorgaben zu halten, insbesondere soweit diese in Konflikt

mit US-Recht stehen. In diesem Zusammenhang ist allerdings darauf hinzuweisen, dass eine Vielzahl von Vorgaben des US-Rechts ebenfalls außerhalb der USA Wirkung entfalten. Auch insofern wäre es ein schlechtes Signal, wenn die Datenschutzgrundverordnung auf Grund des inhaltlichen Widerstands einiger Mitgliedstaaten im EU-Rat scheitern würde.

### **Durch welche technischen und organisatorischen Maßnahmen lässt sich die Überwachung verhindern?**

Beim Versuch, den Zugriff AND auf innerdeutsche und europäische Telekommunikationsverkehre durch Rechtsinstrumentarien verschiedener Ebenen zu verhindern, kann es jedoch nicht bleiben. Erforderlich ist auch die Implementierung technisch-organisatorischer Maßnahmen, welche die Überwachung durch AND und sonstige Unbefugte zumindest stark erschweren. Hier denke ich etwa an die sichere Verschlüsselung von Telekommunikationsverkehren, die für möglichst breite Bevölkerungsschichten handhabbar und verständlich sein muss. Zudem beobachte ich mit großem Interesse Überlegungen, innerdeutsche Telekommunikationsverkehre nur noch über in Deutschland gelegene Server zu leiten. Die technische Machbarkeit und Funktionalität solcher Routinglösungen muss schnellstmöglich geklärt werden. Eine weitere Möglichkeit sehe ich in der Stärkung von Datenspeicherkapazitäten innerhalb der EU („European Cloud“ oder „Schengen Cloud“), welche die Abhängigkeit von Privatpersonen und Unternehmen von US-amerikanischen Internetdiensten minimieren und zugleich die technischen Zugriffsmöglichkeiten von AND aus Drittstaaten deutlich verringern würde.

Alle skizzierten Überlegungen zielen auf eine Stärkung der deutschen und europäischen Fähigkeiten zur Weiterentwicklung sicherer und zugleich handhabbarer Kommunikation im Internet ab. Die insbesondere von den USA ausgehende Überwachungs- und Ausspähpraxis zeigt, dass solche Bemühungen kein Selbstzweck etwa um die Stärkung der heimischen IT-Industrie willen sind, sondern letztlich dem Schutz der Kommunikationsgrundrechte dienen.

### **Betroffenheit der Wirtschaft?**

Von der massenhaften Überwachung von Verkehrs- und Inhaltsdaten deutscher Kommunikation sind nicht nur viele Millionen Bürgerinnen und Bürger in ihrem Kommunikationsverhalten und damit ihrer privaten Lebensgestaltung betroffen. Auch die Wirtschaft insgesamt ist in ihrem Vertrauen in die Sicherheit ihrer Kommunikation erschüttert. Es wird befürchtet, dass AND ihre technischen Fähigkeiten auch gezielt dazu nutzen, Wirtschaftsspionage zu betreiben und Betriebs- und Geschäftsgeheimnisse deutscher Unternehmen ausforschen.

Andererseits basieren die Geschäftsmodelle verschiedener Internetunternehmen (etwa Google und Facebook) auf der Sammlung möglichst großer Datenmengen und deren monetärer Nutzung. Die von den Unternehmen angesammelten ungeheuren Datenmengen wecken bei Nachrichtendiensten Begehrlichkeiten. Es kann als gesichert gelten, dass die NSA auf Basis ihrer nach US-Recht bestehenden Zugriffs- und Überwachungsbefugnisse Kenntnis einer Vielzahl von Kundendaten erhalten hat. Zudem wird glaubwürdig darüber berichtet, dass von den betreffenden Unternehmen getroffene IT-Sicherheitsmaßnahmen, insbesondere die Verschlüsselung der Daten bei ihrer Übertragung in internen Netzen, ausgehebelt wurden.

Diesem Risiko müssen Unternehmen u. a. durch vermehrte Investitionen in Datensicherheit begegnen und Datensparsamkeit üben, damit die für Zugriffe von AND verfügbaren Datenmengen reduziert werden.

## **D. Schlussfolgerungen**

Aus meiner Sicht besteht Handlungsbedarf in mehrfacher Hinsicht:

1. Die Bundesregierung ist nach wie vor in der Pflicht, die Sachlage umfassend aufzuklären und den Bundestag ebenso umfassend und laufend über die Ergebnisse ihrer Bemühungen zu informieren. Diese Aufklärungspflicht sehe ich insbesondere im Hinblick auf Art, Umfang und Intensität der Zusammenarbeit der deutschen Nachrichtendienste (ND) mit AND, was die Überwachung des Telekommunikationsverkehrs mit Bezug zu Deutschland angeht und im Hinblick auf die einseitige Tätigkeit von AND mit Bezug zu Deutschland. Ich werde weiterhin nach Kräften selbst an der Aufklärung mitwirken und erwarte dabei die Unterstützung der Bundesregierung und der ihr nachgeordneten Stellen.
2. Der Bundestag muss in die Lage versetzt werden, seinen Gestaltungs- und Kontrollauftrag im Hinblick auf ND-Tätigkeiten angemessen auszuüben. Das Parlamentarische Kontrollgremium und die G10-Kommission fungieren insoweit im Auftrag des Bundestags und lassen sich auf seine verfassungsrechtliche Autorität zurückführen. Im Hinblick auf die komplexen technologischen, fachlichen und praktischen Fragen sollten diese Gremien in die Lage versetzt werden, durch eigenes oder hinzugezogenes externes Know-how die Wahr-

nehmung ihrer Kontrollaufgaben zu optimieren. Ich verweise in diesem Zusammenhang darauf, dass der Bundestag bereits nach geltendem Recht die Beratung und Sachkunde meiner Dienststelle jederzeit in Anspruch nehmen kann. Er kann nicht nur gemäß § 26 Abs. 2 Satz 1 BDSG Gutachten bzw. Berichte anfordern und mich auch ersuchen, „Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes“ nachzugehen (vgl. § 26 Absatz 2 Satz 2 BDSG). Nach § 15 Absatz 5 Satz 3 G 10 kann die G 10-Kommission dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit außerdem Gelegenheit zur Stellungnahme in Fragen des Datenschutzes geben.

3. Die Tätigkeit der die ND kontrollierenden Organe muss effizient und lückenlos ineinandergreifen. Dies ist bis dato nicht der Fall; es bestehen faktisch erhebliche kontrollfreie Räume. Die Kontrolle der G 10-Kommission ist auf die Anordnung von G 10-Maßnahmen und auf die Erhebung, Verarbeitung und Nutzung der durch G 10-Maßnahmen erlangten personenbezogenen Daten beschränkt, während sich meine Kontrollbefugnis nur auf den Umgang mit personenbezogenen Daten außerhalb der nachrichtendienstlichen Telekommunikationsüberwachung erstreckt. Maßnahmen, die auf Erkenntnisse aus der nachrichtendienstlichen Telekommunikationsüberwachung zurückgehen, die aber ihrerseits zur Erhebung und Verarbeitung weiterer personenbezogener Daten führen, sind weder von der G 10-Kommission noch durch mich effektiv überprüfbar. Ich sehe hier akuten gesetzgeberischen Handlungsbedarf zur Optimierung der Kontrollstrukturen.
4. Die Bundesregierung ist verpflichtet, die Grundrechte der Bürger zu schützen. Dies bedeutet im vorliegenden Zusammenhang auch, den Bürgern wirksame und verständliche Mittel an die Hand zu geben, um private Telekommunikation zu schützen. Die Herstellung und Fortentwicklung von IT-Sicherheit darf keinesfalls als alleinige Aufgabe der Bürger angesehen werden. Die Bundesregierung hat insoweit eine Bringschuld, die sie erfüllen muss. Zudem sind Unternehmen, welche Telekommunikationsdienstleistungen und Internetdienste erbringen, verstärkt in die Pflicht zu nehmen, für die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der dabei verarbeiteten Daten zu sorgen und die Daten vor Zugriffen aus Drittstaaten zu schützen. Die derzeit diskutierte EU-Verordnung zum Datenschutz (Datenschutz-Grundverordnung) bietet hierfür einen guten Ansatzpunkt.
5. Die Bundesregierung muss bei allen Maßnahmen (Rechtsetzung, Rechtsänderung, Verhandlungen mit AND, sonstige Aktivitäten auf internationaler Ebene etc.) den Bundestag und die Kontrollorgane eng, umfassend, unaufgefordert und fortlaufend einbeziehen. Für das Gemeinwesen steht zu viel auf dem Spiel, als dass darauf verzichtet werden dürfte, jetzt alle nationalen Ressourcen zu bündeln.
6. Nachrichtendienstliche Tätigkeit muss rechtsstaatlich und daher effektiv kontrollierbar sein. Das gilt auch für die Zusammenarbeit deutscher Dienste mit ihren ausländischen Partnern. Eine solche Zusammenarbeit – so notwendig sie im Einzelfall für die Gewährung von Sicherheit sein mag – darf etwa durch „geschickte“ Aufgabenteilung nicht dazu führen, dass nationale (verfassungs-)rechtliche Beschränkungen umgangen werden. Der Aufbau eines internationalen Regelungs- und Kontrollregimes ist daher dringend geboten. Daher fordere ich die Bundesregierung auf, diese Zusammenarbeit – und ihre Grenzen – in völkerrechtlichen bereichsspezifischen Verträgen zu regeln. Dies würde dem Bundestag durch seinen Einfluss auf das Verhandlungsmandat für die Bundesregierung entscheidenden Einfluss auf das Verhandlungsergebnis sichern. Ferner obläge es seiner Entscheidungsgewalt, den Vertrag zu ratifizieren, um ihn in geltendes Bundesrecht zu überführen. Zudem halte ich es für geboten, dass die Bundesregierung auch über Verhandlungen, Abkommen und Verabredungen unterhalb verbindlicher völkerrechtlicher Vorgaben die erforderliche Transparenz herstellt und für entsprechende parlamentarische Einflussmöglichkeiten sorgt.
7. Angesichts der bekannt gewordenen Aktivitäten der Nachrichtendienste von EU-Mitgliedstaaten (etwa im Rahmen des Programms „Tempora“ des britischen Geheimdienstes GCHQ) halte ich einen gemeinsamen europäischen Rechtsrahmen für nachrichtendienstliche Überwachungsmaßnahmen für erforderlich. Dieser Rechtsrahmen müsste durch völkerrechtliche Verträge geschaffen werden, da die EU hier keine Rechtssetzungsbefugnis hat. Ein erster Schritt könnte in einer Art grundrechtlichen „Meistbegünstigungsklausel“ bestehen, nach der sich die beteiligten Staaten verpflichten, die Schutzvorkehrungen, die nach nationalem Recht den eigenen Staatsbürgern und dort ansässigen Ausländern zustehen, auch auf die Bürger der übrigen Staaten zu erstrecken.