universitätbonn

Rheinische Friedrich-Wilhelms-Universität Bonn
Institut für Völkerrecht
Direktor
Prof Dr S Talmon LLM MA

universität bonn · Institut für Völkerrecht · Adenauerallee 24-42 · 53113 Bonn

An den Vorsitzenden des
1. Untersuchungsausschuss der 18. WP
Herrn Prof. Dr. Patrick Sensburg, MdB
Deutscher Bundestag
Platz der Republik 1

11011 Berlin

Deutscher Bundestag
1. Untersuchungsausschuss
03. Juni 2014

Deutscher Bundestag
1. Untersuchungsausschuss
der 18. Wahlperiode

MAT A SV-4/2

zu A-Drs.: 56

Adenauerallee 24-42,
D 53113 Bonn
Tel.: +49(0)228/73-91 72
Tel.: +49(0)228/73-39 32
Fax: +49(0)228/73-91 71
talmon@jura.uni-bonn.de

Bonn, 2.06.2014

Sachverständigengutachten gemäß Beweisbeschluss SV-4 des 1. Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode

Sehr geehrter Herr Vorsitzender,

anbei übersende ich Ihnen das vom 1. Untersuchungsausschuss des Deutschen Bundestages für die 18. Wahlperiode angeforderte Sachverständigengutachten gemäß Beweisbeschluss SV-4 vom 10. April 2014.

Ich habe mich in meinen schriftlichen Ausführungen auf den völkerrechtlichen Teil der Leitfragen konzentriert. Zum europarechtlichen Teil der Leitfragen bin ich – im Rahmen meiner Kompetenz – gerne bereit, im Rahmen der mündlichen Anhörung Ausführungen zu machen.

Mit freundlichen Grüßen
Ihr
Stefan Talmon

Anlage

universitätbonn

Rheinische Friedrich-Wilhelms-Universität Bonn

Institut für Völkerrecht
Direktor
Prof Dr S Talmon LLM MA

universität **bonn** · Institut für Völkerrecht · Adenauerallee 24-42 · 53113 Bonn

Adenauerallee 24-42,
D 53113 Bonn
Tel.: +49(0)228/73-91 72
Tel.: +49(0)228/73-39 32
Fax: +49(0)228/73-91 71
talmon@jura.uni-bonn.de

Bonn, 2.6.2014

Sachverständigengutachten gemäß Beweisbeschluss SV-4 des 1. Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode

I. Völkerrechtliche Regelungen über die Erhebung, Speicherung, Auswertung und den Austausch von Daten

1. Leitfrage: Welche völkerrechtlichen Normen (jeweils multilateral, bilateral, Völkergewohnheitsrecht und insbesondere EMRK) gelten für bzw. erfassen Erhebung, Speicherung auf Vorrat, Auswertung und Austausch von Daten aus und über Telekommunikationsvorgängen und Internetnutzung? Gibt es dabei Unterschiede zwischen Daten privater und staatlicher Nutzer?
Gibt es im Völkerrecht Normen zum Schutz privater Nutzer von Telekommunikation und Internet gegenüber staatlichen Stellen oder gegenüber den Betreibern von Infrastruktur für Telekommunikation und Internet?

1. Spezielle Regelungen zum Datenschutz

2. Einen universellen multilateralen Vertrag zum Datenschutz gibt es ebenso wenig wie von der Bundesrepublik Deutschland geschlossene bilaterale Verträge in diesem Bereich.[1] Fragen des Datenschutzes werden jedoch in Spezial- und Regionalabkommen geregelt. Zu nennen ist hier z.B. die Konstitution und Konvention der Internationalen Fernmeldeunion, die u.a. eine Regelung des Fernmeldegeheimnisses enthält.[2] Die Mitglieder der Fernmeldeunion (darunter die Bundesrepublik Deutschland sowie die Staaten der sog. „Five Eyes") verpflichten sich darin, „alle nur möglichen Maßnahmen zu treffen [...], um die Geheimhaltung der Nachrichten im internationalen Verkehr zu gewährleisten".[3] Der Vertrag begründet lediglich eine Pflicht der Vertragsparteien; Rechte des Einzelnen auf ein Fernmeldegeheimnis lassen sich daraus nicht ableiten. Das Fernmeldegeheimnis steht zudem unter dem Vorbehalt, dass die Staaten „den zuständigen Behörden von diesem Nachrichtenverkehr Kenntnis" geben, um die Anwendung ihrer innerstaatlichen Rechtsvorschriften zu sichern.[4]

3. Im Rahmen des Europarates wurde 1981 ein sog. „Datenschutz-Übereinkommen" geschlossen, das auch Nichtmitgliedstaaten des Europarats zum Beitritt offensteht.[5] Zweck des Übereinkommens ist es, „im Hoheitsgebiet" jeder Vertragspartei für jedermann

---

[1] Eine datenschutzrechtliche Bestimmung findet sich jedoch z.B. in Art. 2 des Abkommens zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Republik Ungarn über die gegenseitige Vertretung bei der Visabearbeitung und der Erfassung biometrischer Daten durch ihre diplomatischen und konsularischen Vertretungen v. 18.9.2008 (BGBl. 2008 II S. 1331).
[2] Konstitution und Konvention der Internationalen Fernmeldeunion v. 22.12.1992 (BGBl. 1996 II S. 1306).
[3] Ebd., Art. 37 Abs. 1.
[4] Ebd., Art. 37 Abs. 2.
[5] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten („Datenschutzübereinkommen") v. 28.1.1981 (BGBl. 1985 II S. 539). Das Übereinkommen ist für die Bundesrepublik Deutschland seit 1.10.1985 und für das Vereinigte Königreich seit 1.12.1987 in Kraft. Andere

ungeachtet seiner Staatsangehörigkeit und seines Wohnortes sicherzustellen, dass sein Recht auf einen Persönlichkeitsbereich bei der automatischen Verarbeitung personenbezogener Daten geschützt wird („Datenschutz“).[6] Die Vertragsparteien sind verpflichtet, das Übereinkommen auf automatisierte Dateien/Datensammlungen und automatische Verarbeitungen von personenbezogenen Daten im öffentlichen und privaten Bereich anzuwenden.[7] Es erstreckt sich damit grundsätzlich auch auf die Datensammlungen der Nachrichtendienste der Vertragsparteien. Das Übereinkommen legt in Artikel 5 bis 8 materielle „Grundsätze für den Datenschutz“ fest. Die Vertragsparteien sind verpflichtet, in ihrem innerstaatlichen Recht die erforderlichen Maßnahmen zu treffen, um diese Grundsätze zu verwirklichen.[8] Das Übereinkommen statuiert eine Pflicht zur Gesetzgebung und richtet sich an die Vertragsstaaten. Der Einzelne kann kein Recht auf Datenschutz aus dem Vertrag herleiten.[9] Zudem ist es den Vertragsparteien gestattet, in ihrem nationalen Recht solche Ausnahmen und Einschränkungen von den Grundsätzen des Datenschutzes vorzusehen, die in einer demokratischen Gesellschaft „zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten“ notwendig sind.[10] Der Begriff „Sicherheit des Staates“ soll nach den Erläuterungen zum Vertrag als „*in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State*“ verstanden werden.[11] Die Bezugnahme auf „in einer demokratischen Gesellschaft“ notwendige Maßnahmen lehnt sich an die Bestimmungen der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) an. Die Zulässigkeit von Ausnahmen ist danach einer Verhältnismäßigkeitsprüfung zu unterziehen. Dabei richtet sich die Notwendigkeit einer Maßnahme nicht nach einheitlichen Maßstäben, sondern ist im Lichte der Gegebenheiten im jeweiligen Vertragsstaat zu bestimmen.[12]

4. Das Zusatzprotokoll zum Datenschutz-Übereinkommen des Europarats von 2001, das nur für die Bundesrepublik Deutschland, nicht aber die Staaten der „Five Eyes“-Allianz bindend

---

Staaten der „Five Eyes“ werden durch das Übereinkommen nicht gebunden. Uruguay ist der einzige Nichtmitgliedstaat des Europarats, der an das Übereinkommen gebunden ist.

[6] Datenschutzübereinkommen, Art. 1.

[7] Ebd., Art. 3 Abs. 1.

[8] Ebd., Art. 4 Abs. 1.

[9] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – Explanatory Report, § 38, http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm (alle Internetseiten wurden zuletzt am 31.5.2014 abgerufen).

[10] Datenschutzübereinkommen, Art. 9 Abs. 2(a).

[11] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – Explanatory Report, § 56.

[12] Ebd., § 55.

ist,[13] verpflichtet die Vertragsparteien zur Einrichtung von Kontrollstellen, die die Einhaltung der Datenschutzgrundsätze des Übereinkommens im nationalen Recht gewährleisten sollen.[14] Zudem sollen die Vertragsparteien in ihrem innerstaatlichen Recht sicherstellen, dass personenbezogene Daten nur dann an einen Empfänger, der – wie z.B. die National Security Agency (NSA) – der Hoheitsgewalt einer Nichtvertragspartei des Datenschutz-Übereinkommens untersteht, weitergegeben werden dürfen, wenn diese Nichtvertragspartei (USA) ein angemessenes Schutzniveau für die beabsichtigte Datenweitergabe gewährleistet.[15] Gesetzliche Ausnahmen von diesem Erfordernis sind jedoch „wegen berechtigter überwiegender Interessen, insbesondere wichtiger öffentlicher Interessen", zulässig. [16] Ebenso wie das Übereinkommen selbst begründet das Zusatzprotokoll keine Rechte des Einzelnen, sondern verpflichtet lediglich die Staaten zur Gesetzgebung.

5. Verstöße gegen das Datenschutz-Übereinkommen und das Zusatzprotokoll können nur von den Vertragsparteien geltend gemacht werden. Eine Streitbeilegungsklausel enthalten die beiden Verträge nicht. Vertragsverletzungen können gerichtlich nur geltend gemacht werden, soweit die Gerichtsbarkeit internationaler Gerichte durch Zustimmung der Streitparteien begründet ist. Im Verhältnis zwischen der Bundesrepublik Deutschland und dem Vereinigten Königreich ist der Internationale Gerichtshof (IGH) in Den Haag zur Beilegung von Streitigkeiten über das Datenschutz-Übereinkommen zuständig.[17] In einem solchen Streitfall könnte es aber nicht um die Verletzung des Datenschutz-Übereinkommens durch nachrichtendienstliche Tätigkeiten der britischen Dienste in oder gegen die Bundesrepublik Deutschland bzw. deren Bevölkerung gehen, sondern lediglich um die mangelnde oder fehlerhafte Umsetzung des Übereinkommens in britisches Recht.

6. Datenschutzrelevante Bestimmungen enthält auch das im Rahmen des Europarats im Jahr 2001 abgeschlossene Übereinkommen über Computerkriminalität.[18] Das Übereinkommen steht auch Nichtmitgliedstaaten des Europarats zum Beitritt offen und bindet sowohl die Bundesrepublik Deutschland als auch drei der „Five Eyes" (das Vereinigte Königreich, die Vereinigten Staaten von Amerika und Australien). Das Übereinkommen regelt u.a. die Strafbarkeit des „unbefugten Zugangs" zu einem Computersystem und das „unbefugte

---

[13] Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr v. 8.11.2001 (BGBl. 2002 II S. 1887). Das Vereinigte Königreich hat das Zusatzprotokoll unterzeichnet, aber noch nicht ratifiziert.
[14] Ebd., Art. 1.
[15] Ebd., Art. 2 Abs. 1.
[16] Ebd., Art. 2 Abs. 2, 2. Spiegelstrich.
[17] Siehe Europäisches Übereinkommen zur friedlichen Beilegung von Streitigkeiten v. 29.4.1957 (BGBl. 1961 II S. 81), Art. 1(a).
[18] Übereinkommen über Computerkriminalität v. 23.11.2001 (BGBl. 2008 II S. 1243).

Abfangen“ nichtöffentlicher Computerdatenübermittlungen,[19] die Anordnung der Herausgabe von Computerdaten, die Durchsuchung und Beschlagnahme gespeicherter Computerdaten, die Erhebung von Verkehrsdaten und Inhaltsdaten in Echtzeit und die Rechtshilfe beim Zugriff auf Computerdaten sowie bei der Erhebung von Verkehrs- und Inhaltsdaten in Echtzeit.[20] Das Übereinkommen begründet Rechte und (Gesetzgebungs- und Zusammenarbeits-) Pflichten für die Vertragsparteien; Datenschutzrechte des Einzelnen lassen sich daraus nicht ableiten. Das Übereinkommen verpflichtet die Vertragsparteien lediglich, in ihrem innerstaatlichen Recht „einen angemessenen Schutz der Menschenrechte und Freiheiten einschließlich der Rechte vorsehen, die sich aus ihren Verpflichtungen nach dem Übereinkommen des Europarats von 1950 zum Schutz der Menschenrechte und Grundfreiheiten, dem Internationalen Pakt der Vereinten Nationen von 1966 über bürgerliche und politische Rechte und anderen anwendbaren völkerrechtlichen Übereinkünften auf dem Gebiet der Menschenrechte ergeben und zu denen der Grundsatz der Verhältnismäßigkeit gehören muss“, sicherzustellen.[21]

7. Völkergewohnheitsrechtlich verbindliche Regelungen zum Datenschutz existieren mangels entsprechender einheitlicher Staatenpraxis bislang nicht. Von den ca. 200 Staaten haben lediglich 99 ein mehr oder weniger umfangreiches nationales Datenschutzrecht.[22] Auf internationaler Ebene gibt es zwar Richtlinien und Empfehlungen für die Verarbeitung von Daten und den grenzüberschreitenden Datenverkehr,[23] diese sind jedoch rechtlich nicht verbindlich und sehen Ausnahmen im Interesse „der hoheitlichen Gewalt, staatlichen Sicherheit und öffentlichen Ordnung („*ordre public*“)“ vor.[24] Die Rechtsabteilung des Generalsekretariats der Vereinten Nationen hat zwar im Jahr 2006 festgestellt, dass *„[t]he international binding and non-binding instruments, as well as the national legislation adopted by States, and judicial decisions reveal a number of core principles [of data protection]“*,[25] doch erscheint es zweifelhaft, ob diese Grundsätze unter den Staaten tatsächlich breite

---

[19] Das Erfordernis des „unbefugten“ Handelns nimmt nachrichtendienstliche Tätigkeiten in Übereinstimmung mit den nationalen Gesetzen der Vertragsparteien von der Bestrafungspflicht aus.
[20] Siehe ebd., Art. 2, 3, 18, 19, 20, 21, 31, 33, 34.
[21] Ebd., Art. 15 Abs. 1. Siehe auch Convention on Cybercrime – Explanatory Report, §§ 31, 145, 146, 215; http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.
[22] Siehe *Greenleaf*, ‘Global Tables of Data Privacy Laws and Bills, 3rd ed. June 2013’, UNSW Law Research Paper No. 2013-39, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280875.
[23] Siehe z.B. Empfehlung des Rates der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten („OECD-Leitlinien“) v. 23.9.1980, http://www.oecd.org/internet/ieconomy/15589558.pdf; United Nations General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, UN Doc. A/RES/45/95 v. 14.12.1990.
[24] OECD-Leitlinien, Ziff. 4.
[25] Report of the International Law Commission, UN Doc. A/61/10, 2006, Annex D (Protection of Personal Data in Transborder Flow of Information), S. 489, 498 (§ 11).

Unterstützung gefunden haben.[26] Gegen die Annahme gewohnheitsrechtlicher Standards spricht auch, dass die 35. Jahreskonferenz der internationalen Datenschutzbeauftragten im September 2013 die Regierungen aufgerufen hat sich für die Annahme eines Zusatzprotokolls zu Artikel 17 des Internationalen Paktes für bürgerliche und politische Rechte auszusprechen, *„in order to create globally applicable standards for data protection and the protection of privacy in accordance with the rule of law".*[27] Selbst wenn man bereits von einem völkergewohnheitsrechtlichen Bestand an „Grundsätzen" des Datenschutzes ausgehen wollte, gehörte der Grundsatz der Derogation oder Einschränkbarkeit des Datenschutzes im Interesse der nationalen Sicherheit und öffentlichen Ordnung ebenfalls dazu.[28]

2. Menschenrechtliche Regelungen über die Achtung des Privatlebens

8. Das Recht auf Achtung des Privatlebens umfasst das Recht auf Achtung der Privatsphäre und der Korrespondenz, worunter auch das Recht auf Schutz personenbezogener Daten fällt. Datenschutz wird als ein spezifisch ausgestalteter Teilbereich des Rechts auf Achtung der Privatsphäre angesehen. Der Schutzbereich des Rechts auf Achtung des Privatlebens ist immer dann eröffnet, wenn Daten einer Person erhoben, gespeichert, verarbeitet, ausgewertet oder ausgetauscht werden.[29] Der Begriff der persönlichen Daten umfasst jede Information über eine bestimmte oder bestimmbare Person, einschließlich Telefondaten (gewählte Rufnummern, eingegangene Anrufe, Gesprächsdauer, Gesprächsinhalte), Email-Daten (Empfänger, Inhalte) und Internetdaten (IP-Adressen, besuchte Webseiten, Verweildauer).[30] Eingriffe in das Recht auf Privatleben können sowohl beim Gewinnen und Sammeln der personenbezogenen Daten als auch bei deren Speicherung, Verwendung und Austausch vorkommen. So sind geheime Internet- und Telekommunikationsüberwachungsmaßnahmen durch Nachrichtendienste regelmäßig als Eingriff in das Recht auf Privatleben anzusehen.[31]

9. Das Recht auf Achtung des Privatlebens wird in zahlreichen Menschenrechtsverträgen verbürgt. So findet sich das Recht u.a. in Artikel 17 des Internationalen Pakts über bürgerliche

---

[26] Ebenso *Kuner*, 'An International Legal Framework for Data Protection: Issues and Prospects', Computer Law & Security Review 25 (2009), S. 307, 310.

[27] Siehe 35th International Conference of Data Protection and Privacy Commissioners, Resolution on Anchoring Data Protection and the Protection of Privacy in International Law, 26.9.2013, https://privacyconference2013.org/. Die Federal Trade Commission der USA enthielt sich bei der Abstimmung über diese Resolution.

[28] Siehe Report of the International Law Commission, UN Doc. A/61/10, 2006, Annex D (Protection of Personal Data in Transborder Flow of Information), S. 489, 498 (§ 11), 504-505 (§§ 23, 24).

[29] Vgl. z.B. *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, 5. Aufl. 2012, § 22 Rn. 10.

[30] Vgl. *Esser* in: Löwe-Rosenberg, StPO, Band 11: EMRK; IPBPR, 26. Aufl. 2012, Art. 8 EMRK (Art. 17, 23, 24 IPBPR), Rn. 85.

[31] *Grabenwarter/Pabel* (Fn. 29), § 22 Rn. 27; *Nowak*, U.N. Covenant on Civil and Political Rights: CCPR Commentary, 2nd edn. 2005, Article 17, Rn. 48.

und politische Rechte (IPBPR),[32] in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK),[33] in Artikel 16 des Übereinkommens über die Rechte des Kindes,[34] sowie in Artikel 11 Abs. 2 der Amerikanischen Konvention über Menschenrechte (AMRK).[35] Diese Verträge sind nur für die jeweiligen Vertragsparteien bindend. So sind sowohl die Bundesrepublik Deutschland als auch alle Staaten der „Five Eyes"-Allianz an den IPBPR gebunden. Die Vereinigten Staaten von Amerika sind aber weder Vertragspartei der EMRK, noch der Kinderrechtskonvention oder der AMRK. Vertragliche Bindungen können sich für diese also nur aus dem IPBPR ergeben. Das Vereinigte Königreich ist ebenso wie die Bundesrepublik Deutschland dagegen auch Vertragspartei der EMRK und der Kinderrechtskonvention. Im Folgenden soll deshalb der Blick vor allem auf den Artikel 17 des IPBPR und den Artikel 8 der EMRK gerichtet werden.

10. Der Umfang bzw. Inhalt des verbürgten Rechts auf Achtung des Privatlebens bestimmt sich nach dem im Einzelfall anwendbaren Vertrag. So schützt der IPBPR nur die persönlichen Daten natürlicher Personen,[36] wohingegen die EMRK auch die Geschäfts- und anderen Daten juristischer Personen (wie z.B. Wirtschaftsunternehmen) schützt.[37] Die Daten staatlicher Stellen werden weder vom Schutzbereich des IPBPR noch von dem der EMRK erfasst.[38] Die personenbezogenen Daten der Amtsträger selbst werden dagegen wiederum geschützt (wobei im Einzelfall die Abgrenzung zwischen privaten und staatlichen Daten gerade bei Mitgliedern der Regierung und hohen Amtsträgern schwierig sein kann).

11. Die entscheidende Frage für die Anwendbarkeit der beiden Menschenrechtsverträge auf die grenzüberschreitende nachrichtendienstliche Überwachung der Internetnutzung und des Telekommunikationsverkehrs ist deren räumlicher und persönlicher Geltungsbereich (*ratione loci* und *ratione personae*). Nach Artikel 1 EMRK sichern die Hohen Vertragsparteien „allen ihrer Hoheitsgewalt unterstehenden Personen" die in der Konvention niedergelegten Rechte und Freiheiten zu. Artikel 2 Abs. 1 IPBPR verpflichtet jeden Vertragsstaat „die in diesem Pakt anerkannten Rechte zu achten und sie allen in seinem Gebiet befindlichen und seiner Herrschaftsgewalt unterstehenden Personen […] zu gewährleisten."

---

[32] Internationaler Pakt über bürgerliche und politische Rechte (IPBPR) v. 19.12.1966 (BGBl. 1973 II S. 1534).
[33] [Europäische] Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) v. 4.11.1950 (BGBl. 2010 II S. 1198).
[34] Übereinkommen über die Rechte des Kindes v. 20.11.1989 (BGBl. 1992 II S. 192).
[35] Amerikanische Konvention über die Menschenrechte (AMRK) v. 22.11.1969 (1144 UNTS 123). Kanada ist ebenso wie die USA nicht Vertragspartei der AMRK.
[36] *Human Rights Committee*, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add.13, 26.5.2004, S. 4, § 9.
[37] *Grabenwarter/Pabel* (Fn. 29), § 22 Rn. 4.
[38] Vgl. EMRK, Art. 34 Abs. 1 („nichtstaatliche Organisation").

12. Die Vereinigten Staaten von Amerika und einige andere Staaten haben unter Hinweis auf den Wortlaut des Artikels 2 Abs. 1 IPBPR geltend gemacht, dass sich eine Person nur dann auf die Rechte aus dem Bürgerrechtspakt berufen kann, wenn sie sich im Staatsgebiet einer Vertragspartei aufhält *„und"* (zusätzlich) deren Herrschaftsgewalt unterworfen ist, da Situationen (wie die militärische Besetzung) vorstellbar seien, in denen sich eine Person zwar im Hoheitsgebiet eines Staates befinde, aber nicht der Herrschaftsgewalt der Regierung des Staates unterstehe.[39] Danach wäre der IPBPR auf exterritoriales Handeln der Vertragsstaaten nicht anwendbar. Weder der Menschenrechtsausschuss der Vereinten Nationen[40] noch der IGH[41] haben sich dieser Auffassung angeschlossen und gehen stattdessen von der Möglichkeit der exterritorialen Geltung des Bürgerrechtspaktes aus, vorausgesetzt, dass die Person „der Herrschaftsgewalt" des Vertragsstaates untersteht. Voraussetzung für die Anwendbarkeit sowohl des IPBPR als auch der EMRK auf die grenzüberschreitende nachrichtendienstliche Überwachung des Internet- und Telekommunikationsverkehrs ist somit, dass die von der Überwachung betroffenen Privatpersonen der „Herrschaftsgewalt" bzw. der „Hoheitsgewalt" des überwachenden Staates unterstehen. Beide Begriffe haben dabei den gleichen Inhalt, da sie nur unterschiedliche deutsche Übersetzungen des Wortes *„jurisdiction"* im authentischen englischen Vertragstext sind.

13. Für die Anwendbarkeit der beiden Menschenrechtsverträge auf nachrichtendienstliche grenzüberschreitende Überwachungsmaßnahmen der Internetnutzung und des Telekommunikationsverkehrs kommt es somit darauf an, dass die diesen Maßnahmen ausgesetzten Personen „der Hoheitsgewalt" des überwachenden Staates „unterstehen". In der Literatur wird dies zum Teil generell für alle Überwachungsmaßnahmen bejaht.[42] Hier ist jedoch zu unterscheiden, ob die Maßnahmen im Staatsgebiet eines anderen Staates vorgenommen werden (wie z.B. das Abhören des Mobiltelefons der Kanzlerin) oder ob diese im Gebiet des die Überwachung vornehmenden Staates vorgenommen werden (wie z.B. die Speicherung und Verarbeitung von Internetnutzungsdaten auf den Computern der NSA in den Vereinigten Staaten oder das „Anzapfen" von Unterseedatenkabeln im Bereich des britischen Küstenmeers durch das Government Communications Headquarters – QCHQ).

---

[39] Zur Ansicht der USA siehe z.B. United States Department of State, Office of the Legal Adviser, Digest of United States Practice in International Law 2006, 2007, S. 346-349. Siehe auch *Nowak* (Fn. 31), S. 43-44.

[40] *Human Rights Committee*, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add.13, 26.5.2004, S. 4, § 10.

[41] International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, ICJ Reports 2004, S. 136, 178-180 (§§ 108-111).

[42] Siehe z.B. *Milanovic*, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', Harvard International Law Journal (forthcoming), S. 61, http://ssrn.com/abstract=2418485; *Nyst*, 'Interference-Based Jurisdiction Over Violations of the Right to Privacy', EJIL:Talk!, 21.11.2013., http://www.ejiltalk.org/.

14. Im Falle von Maßnahmen außerhalb des eigenen Staatsgebiets (sog. „exterritorialen Maßnahmen“) verlangt sowohl der IPBPR als auch die EMRK, dass sich die betroffene Person in einem Gebiet aufhält über das der Vertragsstaat die „wirksame Gesamtkontrolle“ (*effective overall control*) ausübt, wie im Falle der militärischen Besetzung fremden Staatsgebiets, oder dass sich die Person in der Gewalt oder unter der wirksamen (physischen) Kontrolle (*power or effective control*) des Vertragsstaates befindet, wie im Falle der Entführung einer Person im Ausland durch Agenten einer Vertragspartei.[43] In allen Fällen exterritorialer Ausübung von Hoheitsgewalt, die vom Europäischen Gerichtshof für Menschenrechte (EGMR) bislang anerkannt wurden, hatte diese eine völkerrechtliche Rechtsgrundlage in der Zustimmung, Einladung oder Duldung durch den Territorialstaat bzw. im Besatzungsrecht.[44] Bei der bloßen exterritorialen Überwachung des Datenverkehrs von Personen im Gebiet der Bundesrepublik Deutschland durch die Nachrichtendienste ausländischer Staaten üben diese Staaten, wenn überhaupt nur virtuelle Kontrolle, nicht aber wirksame „physische Gewalt und Kontrolle“ über die Personen in Deutschland aus.[45] Dies erscheint vor dem Hintergrund der Rechtsprechung des EGMR nicht ausreichend zu sein.[46] Insbesondere hat der EGMR der Bestimmung der „Hoheitsgewalt“ ausgehend von der Rechtsverletzung eine Absage erteilt. In seiner *Banković*-Entscheidung hat der Gerichtshof ausgeführt: *„[T]he applicants' notion of jurisdiction equates the determination of whether an individual falls within the jurisdiction of a Contracting State with the question of whether that person can be considered to be a victim of a violation of rights guaranteed by the Convention. These are separate and distinct admissibility conditions, each of which has to be satisfied in the afore-mentioned order, before an individual can invoke the Convention provisions against a Contracting State.“*[47] Wenn man allein aus der Tatsache der Rechtsverletzung auf die Hoheitsgewalt des verletzenden Vertragsstaates schließen könnte (sog. *„cause-and-effect“* Gedanke),[48] könnten die Vertragsstaaten für Rechtsverletzungen weltweit verantwortlich gemacht werden. Dies war jedoch niemals intendiert. Zudem wäre das Erfordernis, dass die betroffene Person „der Hoheitsgewalt“ des Vertragsstaates „unterstehen“ muss, in diesem

---

[43] Siehe *Grabenwarter/Pabel* (Fn. 29), § 17 Rn. 13-15; Nowak (Fn. 31), Article 2, Rn. 29 und *Human Rights Committee*, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add.13, 26.5.2004, S. 4, § 10.

[44] Vgl. ECtHR (Grand Chamber), *Al-Skeini and Others v. United Kingdom*, Application No. 55721/07, Judgment, 7.7.2011, §135.

[45] Ebd., §136 („What is decisive in such cases is the exercise of physical power and control over the person in question“).

[46] So aber z.B. *Peters*, 'Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part II', EJIL: Talk!, http://www.ejiltalk.org/; *Margulies*, 'The NSA in Global Perspective: Surveillance, Human Rights and International Counter-Terrorism', Fordham Law Review 82 (2014), S. 2137-2167 (2150-2152).

[47] ECtHR (Grand Chamber), *Bankvić et al. v. Belgium et al.*, Application No. 52207/99, Decision on Admissibility, 12.12.2001, § 75.

[48] Dieser wurde vom EGMR ausdrücklich verworfen, ebd.

Falle ohne jeden (einschränkenden) Inhalt. Weiterhin wäre die so begründete „Hoheitsgewalt" einzig auf die spezifische Verletzungshandlung beschränkt. Die Verträge gehen aber davon aus, dass die betroffene Person der Hoheitsgewalt generell „untersteht". Nicht jede Verletzung eines EMRK oder IPBPR-Rechts durch einen Vertragsstaat bedeutet somit zwangsläufig, dass die verletzte Person der Hoheitsgewalt des Vertragsstaats untersteht. Diese entspricht auch der Ansicht der Bundesregierung, die im Fall *Weber und Saravia* geltend gemacht hatte, dass eine Person in Argentinien, deren Fernmeldeverkehr vom Bundesnachrichtendienst überwacht wurde, nicht der Hoheitsgewalt der Bundesrepublik Deutschland unterstehe.[49]

15. Auch soweit Maßnahmen der nachrichtendienstlichen Überwachung des Datenverkehrs im Staatsgebiet eines Vertragsstaates vorgenommen werden (z.B. „Anzapfen" von Datenverbindungen, die durch das Hoheitsgebiet des Staates verlaufen; Speicherung auf Vorrat von Daten auf Computern im Staatsgebiet oder Auswertung von Daten) bestehen Bedenken gegen die Anwendbarkeit der beiden Menschenrechtsverträge, sofern – wie im Falle der Auslandsüberwachung – die von der Überwachung betroffenen Personen sich selbst nicht im Staatsgebiet des Vertragsstaates aufhalten. Unzweifelhaft wird bei einer Datenverarbeitung durch Nachrichtendienste „Hoheitsgewalt" ausgeübt. Darum geht es jedoch bei der Frage der Anwendbarkeit der Verträge nicht. Es ist vielmehr erforderlich, dass die von der Datenverarbeitung betroffenen Personen der Hoheitsgewalt des Vertragsstaates „unterstehen". Der EGMR geht von einem territorialen Verständnis von Hoheitsgewalt aus, d.h., dass alle Personen, die sich im Territorium eines Vertragsstaates befinden, dessen Hoheitsgewalt unterstehen. So führte der Gerichtshof im Fall *Ben El Mahi* aus: *„[T]he words "within their jurisdiction" in Article 1 must be understood to mean that a State's jurisdictional competence is primarily territorial and also that jurisdiction is presumed to be exercised normally throughout the State's territory. [...] The Court has found clear confirmation of this essentially territorial notion of jurisdiction in the travaux préparatoires, given that the Expert Intergovernmental Committee replaced the words "all persons residing within their territories" with a reference to persons "within their jurisdiction" with a view to expanding the Convention's application to others who may not reside, in a legal sense, but who are, nevertheless, on the territory of the Contracting States."*[50] Voraussetzung für die Anwendbarkeit der EMRK (und ebenso des IPBPR)[51] ist also, dass sich die von der

---

[49] ECtHR (Third Section), *Weber and Saravia v. Germany*, Application No. 54934//00, Decision on Admissibility, 29.6.2006, ECtHR Reports 2006-XI, § 66. Die Frage war vom Gerichtshof nicht zu entscheiden.

[50] ECtHR (Fifth Section), *Ben El Mahi and Others v. Denmark,* Application No. 5853/07, Decision on Admissibility, 11.12.2006 (Hervorhebung durch den Autor).

[51] *Human Rights Committee*, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add.13, 26.5.2004, S. 4, § 10 („States Parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and

Rechtsverletzung betroffene Person „auf dem Gebiet des Vertragsstaates“ befindet. Der EGMR hat deshalb z.B. die Beschwerde von zwei marokkanischen Staatsbürgern mit Wohnsitz in Marokko, die eine Verletzung ihrer Religionsfreiheit in Dänemark geltend gemacht hatten, mangels eines „Anknüpfungspunktes für die Hoheitsgewalt“ (*jurisdictional link*) zurückgewiesen.[52] Nicht anders aber stellte sich die Situation dar, wenn ein deutscher Staatsbürger mit Wohnsitz in der Bundesrepublik Deutschland eine Verletzung seines Rechts auf Achtung des Privatlebens im Vereinigten Königreich geltend machen würde. Einziger Anknüpfungspunkt hier wie dort wäre die Rechtsverletzung durch einen Hoheitsakt im Staatsgebiet einer Vertragspartei. Ebenso wie im Fall exterritorialer Maßnahmen eines Vertragsstaates wäre die so begründete Hoheitsgewalt auf die Verletzungshandlung beschränkt.[53] Das Erfordernis, dass die betroffene Person „der Hoheitsgewalt“ des Vertragsstaates „unterstehen“ muss, wäre in diesem Falle ohne jeden eigenständigen Inhalt. Anknüpfungspunkt für die Verantwortlichkeit der Vertragsstaaten wäre danach nicht mehr, dass Personen „ihrer Hoheitsgewalt unterstehen“, sondern dass Personen von „ihren Hoheitsakten betroffen“ werden. Ein Verständnis von Hoheitsgewalt, das lediglich an die Rechtsverletzung anknüpft, hätte im Falle der Weitergabe personenbezogener Daten zudem zur Folge, dass die betroffenen Personen automatisch der Hoheitsgewalt jedes Vertragsstaates unterstünden, an den die Daten weitergegeben werden. Zudem würde solch eine weite Auslegung des Erfordernisses, dass Personen der Hoheitsgewalt des Vertragsstaates „unterstehen“, im Falle von global angelegten, weitreichenden Überwachungen des Internet- und Telekommunikationsverkehrs durch die Auslandsnachrichtendienste dazu führen, dass potentiell mehrere Millionen (und im Falle einer Überwachung Chinas oder Indiens sogar Milliarden) Menschen Beschwerdeführer sein könnten.

16. Das Ergebnis, dass der Anwendungsbereich der IPBPR und der EMRK in Bezug auf die Vertragspartei, welche die grenzüberschreitende Überwachung der Internetnutzung und der Telekommunikation vornimmt, nicht eröffnet ist, bedeutet nicht, dass das Recht auf Achtung des Privatlebens für diesen Sachverhalt ohne Bedeutung ist. Sowohl aus Artikel 17 IPBPR als

---

to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party“). Danach ist Voraussetzung für die Anwendbarkeit des IPBPR, dass sich die betroffene Person entweder im Staatsgebiet der Vertragspartei befindet oder unter deren Gewalt und wirksamer Kontrolle steht.

[52] Ebd. Der Entscheidung im Fall *Ben El Mahi* scheint die Entscheidung im Fall *Liberty* entgegenzustehen, in der der EGMR die Verletzung des Rechts auf Achtung des Privatlebens von zwei irischen NGOs mit Sitz in Dublin bejaht hat, deren Telekommunikationsverkehr mit englischen NGOs von den britischen Behörden im Vereinigten Königreich überwacht wurde. Die Frage, ob die irischen NGOs der Hoheitsgewalt des Vereinigten Königreichs unterstehen, war im Verfahren nicht thematisiert worden, wohl auch deshalb nicht, da die ebenfalls Beschwerde einlegenden britischen NGOs unzweifelhaft der britischen Hoheitsgewalt unterstanden; siehe ECtHR (Fourth Section), *Liberty and Others v. United Kingdom*, Application No. 58243/00, Judgment, 1.7.2008.

auch aus Artikel 8 EMRK ergeben sich nicht nur Abwehrrechte des Einzelnen, sondern auch Schutzpflichten der Vertragsparteien.[54] Diese Ansicht wird u.a. von den Vereinigten Staaten von Amerika, dem Vereinigten Königreich und Australien im Hinblick auf Artikel 17 IPBPR nicht geteilt.[55] Die Mehrheit der Staaten, einschließlich der Bundesrepublik Deutschland, und der Menschenrechtsausschuss der Vereinten Nationen gehen dagegen von einer Schutzpflicht aus.[56] Im Falle einer Überwachung von Internetnutzung und Kommunikationsvorgängen von Personen in Deutschland durch ausländische Nachrichtendienste trifft die Bundesrepublik Deutschland damit eine Pflicht, die persönlichen Daten von Personen in Deutschland zu schützen, wenn diese durch Dritte – Private oder auch andere Staaten – beeinträchtigt oder bedroht werden. Die Vertragsstaaten müssen zweckmäßige und angemessene Maßnahmen treffen, um das Recht auf Achtung des Privatlebens zu sichern. Dabei kommt ihnen jedoch ein gewisser Ermessensspielraum zu. Bei der Ermessensausübung sind neben dem Recht des Einzelnen auf Achtung des Privatlebens auch nationale Sicherheitsinteressen mit einzubeziehen.[57] Aus der Schutzpflicht ergibt sich damit nicht zwangsläufig eine Pflicht der Bundesrepublik Deutschland (hier des Generalbundesanwalts), ein Ermittlungs- oder Strafverfahren gegen Mitarbeiter ausländischer Nachrichtendienste einzuleiten. In Frage kommen auch technische Schutzvorkehrungen, gesetzliche und diplomatische Maßnahmen (wie Protestnoten) sowie, bei Vorliegen eines Verstoßes gegen das Völkerrecht, Klagen oder Staatenbeschwerden vor internationalen Gerichten (soweit die dafür notwendige Gerichtsbarkeit begründet ist). Die Initiative der Bundesrepublik Deutschland zusammen mit Brasilien, eine Resolution der Generalversammlung der Vereinten Nationen auf den Weg zu bringen, in der das Recht auf Achtung des Privatlebens für das digitale Zeitalter ergänzt und fortgeschrieben wird, kann bereits als Maßnahme im Rahmen der Schutzpflicht gewertet werden.[58]

17. Selbst wenn man von einer Anwendbarkeit des IPBPR und der EMRK auf Maßnahmen der grenzüberschreitenden Internet- und Telekommunikationsüberwachung durch die Auslandsnachrichtendienste ausginge, bedeutete dies nicht, dass solche Maßnahmen zwangsläufig mit dem Recht auf Achtung des Privatlebens unvereinbar wären. Zwar stellt

---

[53] Siehe oben Rn. 14.
[54] Siehe *Esser* (Fn. 30), Rn. 24; *Grabenwarter/Pabel* (Fn. 29), § 22, Rn. 50, 51, 54. Siehe jüngst auch ECtHR (Third Section), *Jalbă v. Romania*, Application No. 43912/10, Judgment, 18.2.2014, § 27.
[55] Siehe *Nowak* (Fn. 31), Article 17, Rn. 6.
[56] Siehe *Human Rights Committee*, General Comment No. 16: Article 17 (The right of respect of privacy, family, home and correspondence and protection of honour and reputation), 8.4.1988, UN Doc. HRI/GEN/1/Rev.9 (Vol. I), § 9.
[57] Vgl. *Grabenwarter/Pabel* (Fn. 29), § 22, Rn. 50; *Meyer-Ladewig*, EMRK Handkommentar, 3. Aufl. 2011, Artikel 8, Rn. 3.
[58] Siehe dazu auch unten Rn. 51.

jede Erhebung, Speicherung auf Vorrat, Auswertung und Austausch personenbezogener Daten durch die Nachrichtendienste einen Eingriff in den Schutzbereich des Rechts auf Achtung des Privatlebens dar,[59] doch kann ein solcher Eingriff unter bestimmten, von der Rechtsprechung des EGMR entwickelten (und vom Menschenrechtsausschuss der Vereinten Nationen weitgehend übernommenen)[60] Voraussetzungen gerechtfertigt sein. So untersagt Artikel 17 IPBPR nicht jeden, sondern nur den „willkürlichen oder rechtswidrigen" Eingriff in das Privatleben, und Artikel 8 Abs. 2 EMRK sieht ausdrücklich vor, dass eine Behörde in die Ausübung das Recht auf Achtung des Privatlebens eingreifen darf, „soweit der Eingriff gesetzlich vorgesehen 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." Maßnahmen zur Überwachung von Telekommunikation und Internet durch die Nachrichtendienste müssen danach (1) auf gesetzlicher Grundlage erfolgen, (2) einen legitimen Zweck verfolgen und (3) dem Grundsatz der Verhältnismäßigkeit genügen.

18. Voraussetzung für die Rechtmäßigkeit der Überwachungsmaßnahmen ist danach zunächst, dass hierfür eine Rechtsgrundlage im nationalen Recht des überwachenden Staates besteht. Dabei kann es sich sowohl um ein Gesetz im formellen als auch im materiellen Sinn handeln. Die Rechtsgrundlage muss für die betroffenen Personen öffentlich zugänglich sowie inhaltlich hinreichend bestimmt sein, so dass etwaige Eingriffe in das Recht auf Achtung des Privatlebens vorhersehbar sind. Vorhersehbarkeit bedeutet allerdings nicht, dass eine Person genau erkennen können muss, wann Überwachungsmaßnahmen gegen sie ergriffen werden, so dass sie ihr Kommunikationsverhalten anpassen kann, sondern dass das nationale Recht in angemessener Klarheit festlegt, wann und auf welche Art und Weise die staatlichen Behörden die Überwachungsmaßnahmen vornehmen können. Bei Maßnahmen, die, wie das Sammeln, Speichern und Auswerten sowie dem Austausch personenbezogener Daten durch staatliche Stellen, regelmäßig im Geheimen und ohne Kenntnis der Betroffenen stattfinden, werden besonders hohe Anforderungen an die Regelungsdichte und den Regelungsgehalt der gesetzlichen Grundlage gestellt. So müssen die Grenzen der Befugnisse zur Internet- und Kommunikationsüberwachung gesetzlich geregelt sein, d.h. es muss geregelt sein, welche Personen in ihrer Kommunikation überwacht werden dürfen, welche Stellen diese

---

[59] Siehe *Grabenwarter/Pabel* (Fn. 29), § 22, Rn. 27.

[60] Vgl. *Human Rights Committee*, Concluding Observations on the Fourth Report of the United States of America; UN Doc. CCPR/C/USA/CO/4, 24.4.2014, S. 10 (§ 22); *Human Rights Committee*, General Comment No. 16: Article 17 (The right of respect of privacy, family, home and correspondence and protection of honour and reputation), 8.4.1988, UN Doc. HRI/GEN/1/Rev.9 (Vol. I), § 2, 3, 8.

Überwachung durchführen dürfen und wer über die Überwachung entscheidet. Zudem muss geregelt sein, welche Daten erhoben, gespeichert, ausgewertet und ausgetauscht werden dürfen und unter welchen Voraussetzungen (z.B. zur Bekämpfung oder Verfolgung welcher Straftaten) und nach welchen Verfahren dies erfolgt. Weiterhin muss gesetzlich festgelegt sein, in welchem (begrenzten) Zeitraum die Daten erhoben werden dürfen, wie lange diese Daten gespeichert werden dürfen, und unter welchen Voraussetzungen die Daten gelöscht werden können oder müssen. Darüber hinaus muss ein (normalerweise aber nicht notwendigerweise gerichtliches) Verfahren zur Sicherung der Rechte der Betroffenen und zur Kontrolle der staatlichen Behörden vorgesehen sein.[61]

19. Die Überwachungsmaßnahmen müssen ein legitimes Ziel verfolgen. Als legitime Ziele für die Überwachung des Internet- und der Telekommunikation kommen u.a. die „nationale und öffentliche Sicherheit" sowie die „Verhütung von Straftaten" in Betracht.[62] Diese Ziele können es erforderlich machen, personenbezogene Daten zu erheben, zu speichern und an andere Stellen weiterzugeben.[63]

20. Bei der Überprüfung der Verhältnismäßigkeit der Überwachungsmaßnahmen ist eine Abwägung zwischen dem Recht der betroffenen Privatperson auf Achtung ihres Privatlebens und dem öffentlichen Interesse an der Erhebung bestimmter Daten zu treffen. Dabei sind die Art der erhobenen Daten und ihre Bedeutung für den Kernbereich der Persönlichkeit des Betroffenen ebenso zu berücksichtigen wie die gesteigerte Bedrohung demokratischer Gesellschaften durch den internationalen Terrorismus und die organisierte Kriminalität. Den Vertragsstaaten kommt hier, insbesondere bei der Einschätzung von Bedrohungslagen ein nicht unerheblicher Ermessensspielraum zu.[64] Extensive Überwachungsmaßnahmen können demokratische Gesellschaften jedoch nicht nur vor Bedrohungen von außen schützen, sondern diese auch von innen unterminieren und letztendlich zerstören. Der EGMR hat dies im Fall *Klass* wie folgt umschrieben: *„As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. [...] Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of*

---

[61] Siehe dazu im Einzelnen *Grabenwarter/Pabel* (Fn. 29), § 22, Rn. 33-35, sowie speziell für die Überwachung der Telekommunikation ECtHR (Third Section), *Weber and Saravia v. Germany*, Application No. 54934/00, Decision on Admissibility, 29.6.2006, ECtHR Reports 2006-XI, §§ 93-95; ECtHR (Grand Chamber), *Rotaru v. Romania*, Application No. 28341/95, Judgment, 4.5.2000, §§ 52-59.

[62] Vgl. EMRK, Art. 8 Abs. 2.

[63] *Grabenwarter/Pabel* (Fn. 29), § 22, Rn. 37.

undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[65]

21. Geht man entgegen der hier vertretenen Ansicht davon aus, dass auch die strategische Überwachung des internationalen Telekommunikationsverkehrs durch die deutschen Nachrichtendienste dem IPBPR und der EMRK unterliegt, so stellt sich die Frage, ob die deutschen gesetzlichen Grundlagen den Anforderungen für eine rechtmäßige Einschränkung des Rechts auf Achtung des Privatlebens genügen. Hier könnten Bedenken insbesondere im Hinblick auf die mangelnde Vorhersehbarkeit und die Verhältnismäßigkeit der Eingriffe bestehen.[66]

22. Das Recht auf Achtung des Privatlebens kann nicht nur gesetzlich eingeschränkt, sondern unter bestimmten Voraussetzungen im Notstandsfall auch für eine begrenzte Zeit ausgesetzt werden.[67] Eine Aussetzung von Rechten muss jedoch ausdrücklich erklärt werden und muss dem Grundsatz der Verhältnismäßigkeit genügen. Die generelle Bedrohung durch den internationalen Terrorismus rechtfertigt eine solche Aussetzung derzeit nicht.[68]

23. Das Recht auf Achtung des Privatlebens ist auch völkergewohnheitsrechtlich gewährleistet. Es findet sich u.a. in Artikel 12 der Allgemeinen Erklärung der Menschenrechte,[69] einer unverbindlichen Resolution der Generalversammlung der Vereinten Nationen, deren Inhalt heute in weiten Teilen gewohnheitsrechtliche Geltung beigemessen wird.[70] Danach darf niemand „willkürlichen Eingriffen in sein Privatleben" ausgesetzt werden. Die Verbürgung des Rechts im Völkergewohnheitsrecht geht nicht über die vertraglichen Verbürgungen hinaus, sondern bleibt eher hinter diesen zurück.

---

[64] Siehe z.B. *Loideain*, 'Surveillance of Communication Data and Article 8 of the European Convention on Human Rights', in: Gutwirth et al. (Hrsg.), Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges, 2014, S. 183-209 (191, 194).

[65] ECtHR (Plenary), *Klass and Others v. Germany*, Application No. 5029/71, Judgment, 6.9.1978, § 49.

[66] Siehe hierzu die von *Bäcker* in seinem Gutachten für den 1. Untersuchungsausschuss der 18. Wahlperiode geäußerten Bedenken im Hinblick auf die nationale Rechtslage.

[67] Siehe EMRK, Art. 15; IPBPR, Art. 4.

[68] Die Suspendierungserklärung, die das Vereinigte Königreich im Zusammenhang mit den Anschlägen vom 11. September 2001 abgegeben hatte wurde als ungültig betrachtet; siehe United Kingdom, House of Lords, *A (FC) et al. v. Secretary of State for the Home Department*, Judgment, 16.12.2004, [2004] UKHL 56.

[69] Allgemeine Erklärung der Menschenrechte v. 10.12.1948, UN Doc. A/RES/217(A) v. 10.12.1948.

II. Völkerrechtliche Regelung staatlicher Spionagetätigkeit

24. Leitfrage: Inwieweit regeln völkerrechtliche Normen staatliche Spionagetätigkeit?

1. Begriff der Spionage

25. Der Begriff der „Spionage" wird im Völkerrecht nicht definiert.[71] Unter Spionage wird gemeinhin das Beschaffen und Erlangen von militärischen, politischen oder wirtschaftlichen, nicht offen zugänglichen Informationen eines Staates durch staatliche Stellen eines anderen Staates verstanden.[72] Heute wird darunter teilweise auch jede grenzüberschreitende Informationsbeschaffung durch staatliche Stellen subsumiert, unabhängig ob diese gegen einen anderen Staat, eine internationale Organisation, Wirtschaftsunternehmen (sog. „Industriespionage") oder Privatpersonen gerichtet ist. Das Beschaffen der Information wird regelmäßig heimlich oder unter falschem Vorwand erfolgen (kann aber auch offen erfolgen) und muss sich auf nicht allgemein zugängliche Informationen beziehen.[73]

2. Grundsatz: Zulässigkeit der Friedensspionage

26. Die Spionage in Friedenszeiten ist, anders als die Behandlung der Spione im bewaffneten Konflikt,[74] im Völkerrecht nicht ausdrücklich geregelt. Die Staaten und die große Mehrheit in der völkerrechtlichen Literatur gehen davon aus, dass Spionage als solche völkerrechtlich erlaubt ist.[75] Dies wird zum einen mit einem auf der Staatenpraxis und der Rechtsüberzeugung der Staaten (*opinio juris*) basierenden völkergewohnheitsrechtlichen

---

[70] Vgl. *Buergenthal/Thürer*, Menschenrechte, 2010, S. 31; *Peters* (Fn. 46).

[71] Siehe jedoch zum Begriff des „Spions" im Kriegsrecht die Haager Landkriegsordnung v. 18.10.1907 (RGBl. 1910, S. 107), Art. 29; und das I. Zusatzprotokoll zu den Genfer Abkommen v. 8.6.1977 (BGBl. 1990 II S. 1551), Art. 46.

[72] Vgl. *Hinz*, 'Spionage', in: Strupp/Schlochauer (Hrsg.), Wörterbuch des Völkerrechts, Bd. III, 1962, S. 298-300 (298, 300).

[73] Siehe *Langkau*, Völker- und landesrechtliche Probleme der Kriegs- und Friedensspionage, 1970, S. 137-140; *Rauch*, 'Espionage', in: Bernhardt (ed.), Encyclopedia of Public International Law, vol. II, 1995, S. 114-116 (114).

[74] Dazu siehe *Schaller*, 'Spies', in: Wolfrum (ed.), The Max Planck Encyclopedia of Public International Law, vol. IX, 2012, S. 435-438 (436-437).

[75] Siehe *Lafouasse*, L'Espionage dans le Droit International, 2012, S. 25-36 m.w.N.; *Sule*, Spionage, 2006, S. 73 m.w.N.; *Scott*, 'Territorially Intrusive Intelligence Collection and International Law', Air Force Law Review 46 (1999), S. 217-226 (217); *Hollweg*, 'Military Reconnaissance', in: Bernhardt (ed.), Encyclopedia of Public International Law, vol. III, 1997, S. 400-403 (401); *Kanuck*, 'Information Warfare: New Challenges for Public International Law', Harvard International Law Journal 37 (1996), S. 272-292 (276); *Parks*, 'The International Law of Intelligence Collection', in: Moore et al. (eds.), National Security Law, 1990, S. 433 (433-434); *Hinz* (Fn. 72), S. 300. Bereits *Hugo Grotius* sprach von den „Kundschafter[n], die man nach dem Völkerrecht aussenden kann"; siehe *Grotius*, Drei Bücher vom Recht des Krieges und des Friedens, 1625 (deutscher Text und Einleitung von Walter Schätzel, 1950), Buch III, Kapitel XVIII, § 3. Contra z.B. *Peters*, 'Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part I', EJIL: Talk!, 1.11.2013, http://www.ejiltalk.org/, die davon ausgeht, dass Spionage völkerrechtlich verboten ist.

Erlaubnistatbestand,[76] zum anderen mit dem sog. „Lotus-Grundsatz“ begründet,[77] wonach den Staaten aufgrund ihrer Souveränität und der daraus resultierenden Handlungsfreiheit völkerrechtlich alles erlaubt ist, was nicht ausdrücklich verboten ist.[78] Ein Spionageverbot hat sich aber im Völkerrecht nicht herausgebildet. Ein solches könnte sich nur aus zwischenstaatlichen Verträgen oder aus dem Völkergewohnheitsrecht ergeben. Eine Resolution der Generalversammlung der Vereinten Nationen zu Spähangriffen ausländischer Geheimdienste, wie sie von Deutschland und Brasilien im Jahr 2013 initiiert wurde,[79] hat dagegen allenfalls politisches oder moralisches Gewicht. Völkerrechtliche Verträge über ein Spionageverbot wurden in der Literatur immer wieder einmal vorgeschlagen,[80] abgeschlossen wurden solche Verträge bislang jedoch nicht.[81] Die Herausbildung einer die Spionage untersagende Regel des Völkergewohnheitsrechts scheitert daran, dass die Staaten „Spionage als ein legitimes Mittel zur Erlangung von Erkenntnissen für die Lagebeurteilung und die Entscheidungsfindung im politischen Bereich“ ansehen[82] und damit die erforderliche Verbotspraxis und Rechtsüberzeugung für die Herausbildung einer völkergewohnheits-rechtlichen Regel fehlen.

27. Auch die deutschen Gerichte gehen in Anlehnung an den „Lotus-Grundsatz“ davon aus, dass Spionage zulässig ist. So führte das Bundesverfassungsgericht aus: „Es ist das Besondere der Spionage, dass das Völkerrecht sie einerseits nicht verbietet, ihre Bestrafung durch den ausspionierten Staat aber selbst dann zuläßt, wenn der Spion ausschließlich außerhalb dieses Staates gehandelt hat.“[83]

28. Der Bundesgerichtshof hat ebenfalls festgestellt, dass es sich bei der Spionage um „ein völkerrechtlich zulässiges – weil nicht verbotenes – amtliches Handeln von Amtsträgern“ eines anderen Staates handelt.[84] In seiner Entscheidung aus dem Jahr 1991 zur Strafbarkeit

---

[76] Siehe z.B. *Kish*, International Law and Espionage (edited by David Turns), 1995, S. XV. A.A. *Ewer/Thienel*, ‘Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals’, NJW 2014, S. 30-36 (31).
[77] Siehe Permanent Court of International Justice, *The Case of the S.S. ‘Lotus’*, [1927] PCIJ Series A, No. 10, S. 18-19.
[78] So z.B. *Lafouasse* (Fn. 75), S. 28; *Stein/Marauhn*, ‘Völkerrechtliche Aspekte von Informationsoperationen’, Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 60 (2000), S. 1-49 (32-33); *Inkster*, ‘The Snowden Revelations: Myths and Misapprehensions’, Survival: Global Politics and Strategy 56 (2014), S. 51-60 (53, 54); *Langkau* (Fn. 73), S. 164. Siehe auch *Schmahl*, ‘Effektiver Rechtsschutz gegen Überwachungsmaßnahmen ausländischer Geheimdienste?’, JZ 2014, S. 220-228 (221: „weder ausdrücklich erlaubt noch verboten“).
[79] Siehe die VN-Generalversammlung, Resolution Nr. 68/167 v. 18.12.2013 zum ‘Recht auf Privatheit im digitalen Zeitalter’ (UN Doc. A/RES/68/167 v. 21.1.2014). Siehe auch ‘Deutschland und Brasilien arbeiten an Resolution zu NSA’, Frankfurter Allgemeine Zeitung v. 28.10.2013, S. 2.
[80] Siehe z.B. *Wehberg*, ‘L’avenir des conférence de la paix’, Revue Générale de Droit International Public 19 (1912), S. 583-598 (585-586).
[81] *Scott* (Fn. 75), S. 218. Siehe zu den sog. „No Spy-Abkommen“ unten bei Rn. 57-60.
[82] Siehe BVerfGE 92, 277 (329).
[83] BVerfGE 92, 277 (328).
[84] BGHSt 37, 305 (308) = NJW 1991, 929 (930).

der DDR-Spione führte das Gericht aus: „Das Friedensvölkerrecht enthält gegenwärtig keinerlei Regelung über die Strafbarkeit nachrichtendienstlicher Betätigung. Trotz mancher Bemühungen, vertragliche Regelungen zumindest im bilateralen Verkehr einzuführen, ist eine Sonderregelung auf vertraglicher Basis bisher nicht zustande gekommen. Im Völkergewohnheitsrecht hat sich eine zu berücksichtigende Übung, welche geheimdienstliche Tätigkeiten in anderen Staaten erlaubt, untersagt oder auf andere Weise dirigiert oder limitiert, nicht gebildet. Die Spionage stellt sich zwar als kein völkerrechtliches Unrecht dar, sie ist im Krieg und Frieden eine völkerrechtlich ‚legale Handlung'. Den einzelnen Staaten ist aber völkerrechtlich nicht untersagt, die Spionagetätigkeit durch nationale Regelungen mit Strafe zu bewehren."[85]

29. Bei der rechtlichen Beurteilung der Spionagetätigkeit ist zwischen der innerstaatlichen und der völkerrechtlichen Ebene zu unterscheiden. Weil ein Verhalten nach nationalem (Straf-)Recht bestraft werden darf, muss das Verhalten auf internationaler Ebene nicht verboten sein.[86] Dem ausgespähten Staat steht es aufgrund seiner Souveränität und der sich daraus ergebenden Handlungsfreiheit frei, die Spionage für ausländische Geheimdienste unter Strafe zu stellen, wie dies im Strafgesetzbuch geschehen ist.[87] Dabei kann das deutsche Strafrecht auf der Grundlage des Schutzprinzips (*protective principle*) auch auf Handlungen, die von ausländischem Territorium ausgehen, ausgedehnt werden.[88]

30. Da die Spionage als solche völkerrechtlich nicht verboten ist, stellt sie auch kein völkerrechtliches Delikt dar.[89] Deutschland kann deshalb z.B. wegen der Späh-Aktionen der NSA von den Vereinigten Staaten von Amerika weder eine förmliche Entschuldigung als Wiedergutmachung fordern noch Gegenmaßnahmen ergreifen.[90] Eine zeitweilige Suspendierung des SWIFT-Abkommens von 2010 zwischen den Vereinigten Staaten von Amerika und der Europäischen Union, das US-Terrorfahndern den Zugriff auf Kontobewegungen von Verdächtigen in der EU erlaubt, wie jüngst vom Europaparlament gefordert,[91] wäre als Reaktion auf die Handlungen der NSA völkerrechtlich unzulässig.

---

[85] Ebd.
[86] Siehe *Lafouasse* (Fn. 75), S. 29-30.
[87] Vgl. § 99 StGB.
[88] Siehe z.B. *Oliver*, 'The Jurisdiction (Competence) of States, in: Bedjaoui (ed.), International Law: Achievements and Prospects, 1991, S. 307-326 (316); *Krizek*, 'The Protective Principle of Extraterritorial Jurisdiction: Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice', Boston University International Law Journal 6 (1988), S. 337-359.
[89] *Lafouasse* (Fn. 75), S. 27; *Doehring*, Völkerrecht, 2. Aufl. 2004, Rn. 1159; *Hinz* (Fn. 72), S. 300.
[90] Vgl. Art. 37 und Art. 49 der Artikel der Völkerrechtskommission der Vereinten Nationen zur Verantwortlichkeit der Staaten für völkerrechtswidrige Handlungen, abgedruckt als Anhang zur Resolution der Generalversammlung der Vereinten Nationen Nr. 56/83, UN Doc. A/RES/56/83 v. 1212.2001.
[91] Siehe 'Europaparlament verlangt Aussetzung des Swift-Abkommens', Frankfurter Allgemeine Zeitung v. 24.10.2013, S. 5.

3. Verstoß gegen die territoriale Souveränität?

31. Soweit in der Literatur zum Teil von einem Verbot der Spionage ausgegangen wird, wird dies mit einem Verstoß gegen die territoriale Souveränität des ausgespähten Staates begründet.[92] Territoriale Souveränität bedeutet, dass die Hoheitsgewalt eines Staates innerhalb seines Staatsgebiets ausschließlich ist, d.h. dass kein Staat im Gebiet eines anderen Staates ohne dessen Erlaubnis Hoheitsgewalt ausüben darf.[93] Die Spionagetätigkeit durch ausländische Amtsträger innerhalb des Staatsgebietes wird als Ausübung von Hoheitsgewalt angesehen, die mit der territorialen Souveränität des ausspionierten Staates unvereinbar ist.[94] Gleiches gilt für Aufklärungsflüge unbemannter Luftfahrzeuge („Spionagedrohnen") im Luftraum eines Staates.[95]

32. Diese Ansicht verkennt jedoch, dass nicht die Spionage an sich völkerrechtlich verboten ist, sondern das unerlaubte Eindringen des Spions (oder der „Spionagedrohne") in fremdes Staatsgebiet zu See, Land oder in der Luft. Der Verstoß gegen das Völkerrecht ist nicht in der Spionagetätigkeit an sich, sondern in der kollateralen Verletzung der territorialen Souveränität zu sehen.[96] Soweit die Spionagetätigkeit kein Eindringen des Spions in das fremde Staatsgebiet erfordert, da sie mit technischen Hilfsmitteln vom Gebiet des spionierenden Staates aus oder von staatsfreien Räumen wie der Hohen See oder dem Weltraum aus durchgeführt wird, liegt kein Verstoß gegen das Völkerrecht vor. Für die völkerrechtliche Zulässigkeit der Spionagetätigkeit ist somit auf die Art und Weise der Tätigkeit bzw. den Ort, von dem aus spioniert wird, abzustellen.[97]

33. Telefonate, Emails oder SMS, die über das Mobilfunknetz abgewickelt werden, können über Spionagesatelliten im Weltall mit angeschlossenen Bodenstationen im Ausland (*remote sensing* oder *peripheral reconnaissance*) „abgefangen" werden. Emails und Daten, die über Computer oder Smartphone versandt werden, oder Telefonate, die über Computer abgewickelt werden (Skype-Gespräche), können auf im Ausland stehenden Servern der Internet-Service-Provider „abgefischt" werden. Zudem wird ein Großteil des weltweiten Datenverkehrs über Glasfaserkabel abgewickelt, die auf dem Meeresboden unter der Hohen See verlaufen. Diese Kabel können „angezapft" und die Daten „umgeleitet" werden. Solche Vorgehensweisen ohne physischen Inlandsbezug verstoßen nicht gegen das

---

[92] Siehe z.B. *Wright*, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs', in: Stanger (ed.), Essays on Espionage and International Law, 1962, S. 3-28 (12).
[93] Siehe Permanent Court of International Justice, *The Case of the S.S. 'Lotus'*, [1927] PCIJ Series A, No. 10, S. 18.
[94] Vgl. *Ewer/Thienel* (Fn. 76), S. 31. Siehe auch *Kish* (Fn. 76), S. 83-101.
[95] Siehe z.B. die Protestnote des Iran, UN Doc. A/66/599–S/2011/764 (9.12.2011).
[96] Siehe *Lafouasse* (Fn. 75), S. 27-28.
[97] *Lafouasse* (Fn. 75), S. 34, 36.

völkergewohnheitsrechtliche Gebot der Achtung der territorialen Souveränität der Staaten.[98] Im Jahr 2006 stellte der Europäische Gerichtshof für Menschenrechte im Hinblick auf die strategische internationale Überwachung des drahtlosen Fernmeldeverkehrs durch den Bundesnachrichtendienst fest, dass das Abhören von Telefonaten im Ausland, die nicht über das Festnetz, sondern über Satellit oder Richtfunkstrecken abgewickelt werden, und die Verwendung der so erlangten Informationen nicht gegen die völkerrechtlich geschützte territoriale Souveränität anderer Staaten verstößt, solange die vom ausländischen Territorium ausgesandten Funksignale von Deutschland aus überwacht und abgefangen werden und die so gesammelten Informationen in Deutschland genutzt werden.[99] Nichts anderes aber machen die NSA oder GCHQ, wenn sie deutsche Regierungsmitglieder oder die Bevölkerung in der Bundesrepublik Deutschland von ihren Einrichtungen in den USA oder im Vereinigten Königreich aus überwachen.

4. Verstoß gegen das Interventionsverbot?

34. In der Literatur wird teilweise auch die Ansicht vertreten, dass Spionage gegen das völkergewohnheitsrechtliche Interventionsverbot verstoße und deshalb rechtswidrig sei.[100] Das Interventionsverbot folgt aus dem Grundsatz der souveränen Gleichheit der Staaten. Die Staaten sollen danach ihre inneren und äußeren Angelegenheiten ohne Einmischung anderer Staaten regeln können.[101] Das Interventionsverbot schützt die Willensfreiheit der Staaten.

35. Diese Ansicht verkennt, dass Wesensmerkmal des Interventionsbegriffs der Zwangscharakter ist.[102] Der Staat muss durch die Zwangsmaßnahme der Kontrolle über seine Angelegenheiten beraubt werden. Schlicht und einfaches Einmischen (*interference*) erfüllt nicht den Tatbestand der Intervention (*intervention*).[103] So hat der Internationale Gerichtshof festgestellt: *„Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed*

---

[98] *Stein/Marauhn* (Fn. 78), S. 33; *Kanuck* (Fn. 75), S. 276, 279-280, 290-291; *Classen*, Fernerkundung und Völkerrecht, 1987, S.126.

[99] ECtHR (Third Section), *Weber and Saravia v. Germany*, Application No. 54934/00, Decision on Admissibility, 29.6.2006, ECtHR Reports 2006-XI, para. 88. Siehe auch *Karg*, Völkerrechtliche Probleme eines Höhenflugs, Jura 2003, S. 129 (132); *Sule* (Fn. 75), S. 85; *Ewer/Thienel* (Fn. 76), S. 31.

[100] *Wright* (Fn. 92), S. 13; *Fleck*, 'Individual and State Responsibility for Intelligence Gathering', Michigan Journal of International Law 28 (2007-2008), 687-709 (692); *Ewer/Thienel* (Fn. 76), S. 31-32. Siehe auch *Jackamo*, 'From the Cold War to the New Multilateral World Order: The Evolution of Covert Operations and the Customary International Law of Non-Intervention', Virginia Journal of International Law 32 (1991-1992), S. 929-977 (935), der davon ausgeht, dass es sich bei Spionage um Intervention handeln könne, diese aber nicht rechtswidrig sei.

[101] Vgl. *Ipsen*, Völkerrecht, 6. Aufl. 2014, §51, Rn. 41.

[102] Siehe *Jamnejad/Wood*, 'The Principle of Non-intervention', Leiden Journal of International Law 22 (2009), S. 345-381 (348).

[103] *Jennings/Watts* (eds.), Oppenheim's International Law, 9. Aufl. 1992, S. 432.

forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State."[104]

36. Nicht jede Verletzung der territorialen Souveränität eines Staats stellt somit eine verbotene Intervention dar. So ist die Ausübung von Hoheitsakten auf fremdem Staatsgebiet ohne Zustimmung der Regierung dieses Staates zwar eine Verletzung seiner territorialen Souveränität, nicht jedoch ein Verstoß gegen das Interventionsverbot, wenn damit kein Zwang gegen den Staat ausgeübt wird.[105]

37. Durch die Spionagetätigkeit, d.h. das bloße Sammeln von Informationen, durch Spione im Staatsgebiet des ausspionierten Staates wird keine Zwangswirkung ausgeübt.[106] So hat der IGH im *Nicaragua*-Fall Aufklärungsflüge der Vereinigten Staaten von Amerika über dem Staatsgebiet von Nicaragua zwar als Verletzung von dessen territorialer Souveränität, nicht aber als unzulässige Intervention verurteilt.[107]

38. Soweit technisch-elektronische Überwachungsmaßnahmen von Datenverarbeitungs- und Telekommunikationsvorgängen von außerhalb des Staatsgebiets des ausspionierten Staates vorgenommen werden, kann erst recht nicht von einer Zwangswirkung auf das Verhalten des betroffenen Staates ausgegangen werden.[108]

5. Verstoß gegen das Diplomatenrecht?

39. Spionagetätigkeiten aus diplomatischen Vertretungen ausländischer Staaten in der Bundesrepublik Deutschland heraus[109] verstoßen gegen das Wiener Übereinkommen über diplomatische Beziehungen (WÜD) von 1961. Danach haben die Angehörigen diplomatischer Missionen die Gesetze und anderen Rechtsvorschriften des Empfangsstaats zu beachten und dürfen die Räumlichkeiten der Mission nicht in einer Weise benutzen, die mit den Aufgaben der Mission unvereinbar ist.[110] Zwar gehört zu den Aufgaben diplomatischer Missionen auch die Nachrichtengewinnung über den Empfangsstaat, doch darf diese nur mit rechtmäßigen

---

[104] *International Court of Justice*, Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986, 14, 108 (§ 205).
[105] Siehe *Ipsen* (Fn. 101), §51, Rn. 48.
[106] *Sule* (Fn. 75), 84-85; *Classen* (Fn. 98), S. 162. Siehe auch *Gusy*, 'Spionage im Völkerrecht', NZWehrR 1984, S. 187-199 (193).
[107] Siehe International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, ICJ Reports 1986, S. 14, 51-53 (§§ 87-91); 128 (§ 251); 147.
[108] Ebenso *Peters* (Fn. 75); Sule (Fn. 75), S. 85.
[109] Siehe *Leyendecker/Goetz*, 'Spionageverdacht gegen US-Botschaft', Süddeutsche Zeitung, 25.10.2013, S. 1.
[110] Siehe Wiener Übereinkommen über diplomatische Beziehungen (WÜD) v. 18.4.1961 (BGBl. 1964 II S. 959), Art. 41 Abs. 1 und 3.

Mitteln erfolgen.[111] Das Ausspähen der Kommunikationsvorgänge der Regierung des Empfangsstaates oder seiner Bevölkerung fällt jedoch nicht darunter.[112]

40. Falls die Bundesregierung Beweise für eine gegen deutsches Recht verstoßende Überwachung der Internetnutzung oder des Telekommunikationsverkehrs durch ausländische Botschaften in Deutschland hat, könnte sie die Entsendestaaten u.U. vor dem IGH in Den Haag wegen Verletzung des Diplomatenrechtsübereinkommens verklagen. Die Möglichkeit, einen anderen Staat vor dem IGH zu verklagen, besteht aber immer nur dann, wenn beide Staaten die Gerichtsbarkeit des IGH anerkannt haben. Dies kann in einem speziellen Streitbeilegungsvertrag oder in einer Streitbelegungsklausel eines allgemeinen Vertrages (sog. *„compromissory clause"*), oder auch nach Entstehen der Streitigkeit in einer Streitbeilegungsvereinbarung (sog. *„compromis"*) *ad hoc* geschehen. Im Fall einer Verletzung des Diplomatenrechtsübereinkommens kann sich die Gerichtsbarkeit des IGH aus dem fakultativen Streitbeilegungsprotokoll zum Diplomatenrechtsübereinkommen ergeben, das Streitigkeiten über die Auslegung oder Anwendung des Übereinkommens der obligatorischen Gerichtsbarkeit des IGH unterwirft.[113] Das Streitbeilegungsprotokoll ist derzeit für 69 Staaten in Kraft, darunter auch für die Bundesrepublik Deutschland und die Staaten der sog. „Five Eyes" mit Ausnahme von Kanada.[114]

41. Ein Strafverfahren vor deutschen Gerichten gegen Mitglieder des Personals ausländischer Vertretungen wegen geheimdienstlicher Agententätigkeit wird regelmäßig an der Immunität der Botschaftsangehörigen scheitern.[115] Hier bleibt der Bundesregierung lediglich die Möglichkeit, die der Spionage verdächtigen Personen zur *persona non grata* zu erklären und deren Tätigkeit an der Botschaft damit zu beenden.[116] Darüber hinaus kann die Bundesregierung den Entsendestaat auffordern, den Umfang seines diplomatischen und anderen Personals an der Berliner Botschaft zu reduzieren und den Betrieb von Funkanlagen in der Botschaft untersagen.[117]

---

[111] WÜD, Art. 3 Abs. 1(d).
[112] Vgl. *Forcese*, 'Spies without Borders: International Law and Intelligence Collection', Journal of National Security Law & Policy 5 (2011), S. 179-210 (200); *Doehring* (Fn. 89), Rn. 497
[113] Siehe Art. I des Fakultativ-Protokolls zum Wiener Übereinkommen über diplomatische Beziehungen betreffend die obligatorische Beilegung von Streitigkeiten v. 18.4.1961 (BGBl. 1964 II S. 1018).
[114] Das Fakultativ-Protokoll ist für Deutschland seit 11.11.1964, für die USA seit 13.11.1972, für das Vereinigte Königreich seit 1.9.1964, für Australien seit 26.1.1968 und für Neuseeland seit 23.9.1970 in Kraft.
[115] Vgl. WÜD, Art. 29, 31, 37.
[116] WÜD, Art. 9.
[117] Siehe WÜD, Art. 11, 27 Abs. 1.

6. Verstoß gegen das NATO-Truppenstatut?

42. Spionagetätigkeiten aus Militärstützpunkten verbündeter Staaten in der Bundesrepublik Deutschland heraus verstoßen gegen das NATO-Truppenstatut.[118] Die Streitkräfte verbündeter Staaten, die in Deutschland stationiert sind, haben das Recht, zum Schutz der Truppe und im Rahmen ihrer Bündnisaufgaben gewisse Aufklärungsmaßnahmen durchzuführen.[119] Ein Recht zum Abhören von Regierungsmitgliedern oder von Privatpersonen oder ein Recht zur Überwachung des Internet- und Telekommunikations-verkehrs aus US-amerikanischen oder britischen Militäreinrichtungen in Deutschland heraus haben sie dagegen nicht.[120] NATO-Militärpersonal in Deutschland hat vielmehr die Pflicht, das Recht des Aufnahmestaates zu achten und sich jeder mit dem Geist des Truppenstatuts nicht zu vereinbarenden Tätigkeit, einschließlich der Spionage, zu enthalten.[121] Dies ergibt sich auch aus Artikel VII des Truppenstatuts, wonach die Behörden des Aufnahmestaates das Recht haben, über Mitglieder einer ausländischen Truppe oder eines zivilen Gefolges und deren Angehörige die ausschließliche Gerichtsbarkeit in Bezug auf strafbare Handlungen gegen die Sicherheit des Staates, einschließlich der "Spionage oder Verletzung eines Gesetzes, das sich auf Amtsgeheimnisse dieses Staates" bezieht, auszuüben.[122]

43. Etwas anderes ergibt sich auch nicht aus Artikel 3 Absatz 2 (a) des Zusatzabkommens zum NATO-Truppenstatut, wonach die deutschen Behörden und die Behörden der in Deutschland stationierten verbündeten Truppen bei der Sammlung aller Nachrichten, die für die Sicherheit des Entsendestaates und ihrer Truppen relevant sind, eng zusammenarbeiten.[123] Aus der Pflicht zur geheimdienstlichen Zusammenarbeit bei der Nachrichtensammlung lässt sich kein Recht ausländischer (Militär-)Geheimdienste zum Abhören deutscher Staatsorgane oder der Bevölkerung in Deutschland ableiten. Gleiches gilt für das Recht der in der Bundesrepublik stationierten Truppen, „für militärische Zwecke" Fernmeldeanlagen (außer Funkanlagen) in Deutschland zu errichten, zu betreiben und zu unterhalten und diese an die öffentlichen Fernmeldenetze der Bundesrepublik anzuschließen.[124] Die (sachlich begrenzten)

---

[118] Abkommen zwischen den Parteien des Nordatlantikvertrags über die Rechtsstellung ihrer Truppen (NATO-Truppenstatut) v. 19.6.1951 (BGBl. 1961 II S. 1190), Art. II.
[119] Siehe *Kish*, (Fn. 76), S. 85.
[120] Vgl. *Schmitt*, 'Computer Network Attack: The Normative Software', Yearbook of International Humanitarian Law 2001, 2004, S. 53-85 (59).
[121] NATO-Truppenstatut, Art. II.
[122] NATO-Truppenstatut, Art. VII Abs. 2(c)(ii).
[123] Zusatzabkommen zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen (ZA-NTS) v. 3.8.1959 (BGBl. 1961 II S. 1183, 1218), Art. 3 Abs. 2(a).
[124] ZA-NTS, Art. 60 Abs. 2-4, 7. Siehe dazu auch Verwaltungsabkommen zur Durchführung des Artikels 60 des Zusatzabkommens vom 3. August 1959 in der durch das Abkommen vom 21. Oktober 1971, die Vereinbarung vom 18. Mai 1981 und das Abkommen vom 18. März 1993 geänderten Fassung zu dem Abkommen zwischen

Befugnisse im Rahmen des Zusatzabkommens zum NATO-Truppenstatut sind im Lichte des Truppenstatuts selbst auszulegen und unterliegen den dort niedergelegten Beschränkungen.[125]

44. Streitigkeiten über die Anwendung und Auslegung des NATO-Truppenstatuts und des Zusatzabkommens sind jedoch, anders als Streitigkeiten über das Wiener Diplomatenrechtsübereinkommen, durch Verhandlungen ohne Inanspruchnahme außenstehender Gerichte zu regeln,[126] so dass eine Rechtsverletzung auf diesem Wege nicht effektiv geltend gemacht werden kann.

45. In der Literatur findet sich die Ansicht, dass die NSA-Abhöraktivitäten aus US-Militärstützpunkten in Deutschland heraus eine rechtliche Grundlage im „fortbestehenden Besatzungsrecht" und insbesondere im sog. „Truppenvertrag" von 1954[127] zwischen den Drei Westmächten (Vereinigte Staaten von Amerika, Vereinigtes Königreich und Frankreich) und der Bundesrepublik Deutschland haben.[128] Der Truppenvertrag war als Zusatzabkommen zum Deutschlandvertrag geschlossen worden und regelte Fragen der Stationierung der Truppen der drei Westmächte in der Bundesrepublik Deutschland. Diese Ansicht übersieht, dass der Truppenvertrag mit Inkrafttreten des Zusatzabkommens zum NATO-Truppenstatut am 1. Juli 1963 außer Kraft getreten ist und schon aus diesem Grund keine Rechtsgrundlage für die NSA-Aktivitäten darstellen kann.[129]

46. Im Zusammenhang mit der vermuteten Spionagetätigkeit aus US-Militärstützpunkten in Deutschland heraus werden auch immer wieder die „geheimen Verwaltungsvereinbarungen" zwischen der Bundesregierung und den Regierungen der drei Westmächte aus den Jahren 1968/1969 als Rechtsgrundlage für die NSA-Abhöraktivitäten genannt.[130] Die öffentliche

---

den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen (BGBl. 2000 II S. 1317).

[125] Vgl. auch ZA-NTS, Art. 53 Abs. 1, wonach auch für die Benutzung der Liegenschaften der verbündeten Truppen in Deutschland grundsätzlich das deutsche Recht gilt.

[126] NATO-Truppenstatut, Art. XVI; ZA-NTS, Art. 80A.

[127] Vertrag über die Rechte und Pflichten ausländischer Streitkräfte und ihrer Mitglieder in der Bundesrepublik Deutschland („Truppenvertrag") v. 23.10.1954 (BGBl. 1954 II S. 78).

[128] Siehe *Wolf*, 'Der rechtliche Nebel der deutsch-amerikanischen "NSA-Abhöraffäre"', JZ 2013, S. 1039-1046 (1042-1045). Siehe auch *Deiseroth*, 'Nachrichtendienstliche Überwachung durch US-Stellen in Deutschland – Rechtspolitischer Handlungsbedarf?', ZRP 2013, S. 194-197.

[129] Siehe Vertrag über die Beziehungen zwischen der Bundesrepublik Deutschland und den Drei Mächten („Deutschlandvertrag") v. 26.5.1952, in der Fassung v. 23.10.1954 (BGBl. 1955 II S. 306), Art. 8 Abs. 1(b); und Abkommen über das Außerkrafttreten des Truppenvertrages, des Finanzvertrages und des Steuerabkommens v. 3.8.1959 (BGBl. 1961 II S. 1352), Art. 1. Zum Inkrafttreten des ZA-NTS siehe die Bekanntmachung in BGBl. 1963 II S. 745.

[130] Siehe z.B. der Historiker *Josef Foschepoth* im Interview mit der Deutschen Welle: 'Foschepoth: "Die NSA überwacht mit Erlaubnis"', Deutsche Welle v. 26.7.2013, http://www.dw.de/. Siehe auch dessen Interview mit Zeit Online '"Die USA dürfen Merkel überwachen"', Zeit Online v. 25.10.2013, http://www.zeit.de/. Zu den geheimen Verwaltungsvereinbarungen mit den Westmächten siehe auch *Foschepoth*, Überwachtes Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik, 2012, S. 193-195. Der Text der Vereinbarung mit dem Vereinigten Königreich v. 28.10.1968 findet sich ebd., S. 298-301. Zu den „Geheimabkommen" siehe auch *Deiseroth* (Fn. 128), S. 195.

Empörung über diese Abhöraktivitäten in Deutschland veranlasste die Bundesregierung bereits im August 2013 diese – laut Aussage der Bundesregierung – seit der Wiedervereinigung im Jahr 1990 nicht mehr angewandten Vereinbarungen öffentlichkeitswirksam zu kündigen.[131] Am 2. August 2013 erklärte das Auswärtige Amt: „Im gegenseitigen Einvernehmen ist die Verwaltungsvereinbarung mit den USA [...] damit außer Kraft getreten."[132] Für die Spionageaktivitäten der NSA in Deutschland waren diese Vereinbarungen jedoch ohne Bedeutung. Bei der am 28. Oktober 1968 zwischen der Bundesregierung und der Regierung der Vereinigten Staaten von Amerika geschlossenen Verwaltungsvereinbarung zu dem Gesetz zu Artikel 10 des Grundgesetzes ging es gerade darum, dass mit dem Tage des Inkrafttretens des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 Gesetz – G 10) die amerikanischen Geheimdienste nicht mehr selbst im Gebiet der Bundesrepublik Deutschland Überwachungsmaßnahmen durchführen können sollten.[133] Nach Artikel 10 Absatz 2 Satz 1 des Grundgesetzes dürfen Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses nur auf Grund eines Gesetzes angeordnet werden. Ein solches Gesetz wurde aber erst im August 1968 mit dem sog. „G 10 Gesetz" verabschiedet.[134] Durch dieses „Überwachungsgesetz" wurden die alliierten Vorbehaltsrechte in Bezug auf die Überwachung des Brief-, Post- und Fernmeldeverkehrs in Deutschland abgelöst.[135] Davor konnten die drei Westmächte zunächst aufgrund des Besatzungsrechts und ab 1955 auf der Grundlage ihrer Rechte, die sie sich in Artikel 5 Absatz 2 des Deutschlandvertrages vorbehalten hatten,[136] unbeschränkt den Brief-, Post- und Fernmeldeverkehr in der Bundesrepublik Deutschland überwachen. Bereits 1951 hatte es hierzu eine hitzige Debatte im Deutschen Bundestag gegeben, als bekannt wurde, dass die Westmächte zahlreiche Politiker, Gewerkschaftler und Privatpersonen, darunter den Sohn des

---

[131] Siehe 'Überwachung: Deutschland kündigt Spionageabkommen mit Westalliierten', Zeit Online v. 6.8.2013, http://www.zeit.de/.

[132] 'Abhörvereinbarung gekündigt', Süddeutsche Zeitung v. 3.8.2013, http://newsticker.sueddeutsche.de/.

[133] Der Text der weitgehend inhaltsgleichen Verwaltungsvereinbarung mit dem Vereinigten Königreich findet sich bei *Foschepoth*, (Fn. 130), S. 298-301. Siehe ebd., S. 193-195.

[134] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz) (G 10) v. 13.8.1968 (BGBl. I S. 949). Das Gesetz trat am 14.11.1968 in Kraft.

[135] Vgl. das Schreiben des Auswärtigen Amtes an die Botschaft der Vereinigten Staaten von Amerika v. 27.5.1968 betreffend die Ablösung der alliierten Vorbehaltsrechte zur Überwachung des Post- und Fernmeldeverkehrs, Bestätigung der Verbalnote der US-Botschaft durch das Auswärtige Amt, abgedruckt in *Foschepoth*, (Fn. 130), S. 297-298.

[136] Vertrag über die Beziehungen zwischen der Bundesrepublik Deutschland und den Drei Mächten ('Deutschlandvertrag') v. 26.5.1952, in der Fassung v. 23.10.1954 (BGBl. 1955 II S. 306). Der Vertrag trat am 5.5.1955 in Kraft. Art. 5 Abs. 2 lautet: 'Die von den Drei Mächten bisher innegehabten oder ausgeübten Rechte in Bezug auf den Schutz der Sicherheit von in der Bundesrepublik stationierten Streitkräften, die zeitweilig von den Drei Mächten beibehalten werden, erlöschen, sobald die zuständigen deutschen Behörden entsprechende Vollmachten durch die deutsche Gesetzgebung erhalten haben und dadurch in Stand gesetzt sind, wirksame Maßnahmen zum Schutz der Sicherheit dieser Streitkräfte zu treffen'. Die entsprechenden Vollmachten wurden durch das G 10-Gesetz 1968 geschaffen.

damaligen Bundespräsidenten, abhörten.[137] Gerade diese Praxis sollte durch die Verwaltungsvereinbarungen von 1968/1969 beendet werden. In Zukunft sollten sich die ausländischen Geheimdienste an den deutschen Verfassungsschutz und den Bundesnachrichtendienst wenden, die die Überwachungsaktionen auf der Grundlage des G 10-Gesetzes für die ausländischen Geheimdienste durchführen sollten.[138] Eine Verpflichtung zu dieser geheimdienstlichen „Amtshilfe" ergab sich für Abhörmaßnahmen im Interesse der Sicherheit der Westmächte und zum Schutz ihrer in Deutschland stationierten Truppen aus Artikel 3 Absatz 2 (a) des Zusatzabkommens zum NATO-Truppenstatut.[139] Mit dem Abschluss der Vereinbarungen war aber jedem direkten Abhören durch die NSA (oder den britischen oder französischen Geheimdienst) innerhalb Deutschlands die Grundlage entzogen.

7. Verstoß gegen Menschenrechtsverpflichtungen

47. Spionagetätigkeiten in Deutschland stellen in der Regel keinen Verstoß gegen Menschenrechtsverpflichtungen der Spionage treibenden Staaten dar. Zwar kann die Überwachung der Internetnutzung und der Telekommunikationsvorgänge von Privatpersonen (einschließlich von Regierungsmitgliedern und anderen Amtsträgern) in Deutschland einen Eingriff in das Recht auf Achtung des Privatlebens der betroffenen Personen darstellen, doch scheitert ein Rechtsverstoß bereits am mangelnden örtlichen Anwendungsbereich der einschlägigen Menschenrechtsverträge oder an der fehlenden Rechtswidrigkeit des Eingriffs.[140]

48. Dies soll am Beispiel des Internationalen Paktes über bürgerliche und politische Rechte (Bürgerrechtspakt oder IPBPR) von 1966 erläutert werden.[141] Dieser schützt den Einzelnen in Artikel 17 gegen „willkürliche oder rechtswidrige Eingriffe" in sein „Privatleben".[142] Die IPBPR-Vertragsparteien sind jedoch lediglich verpflichtet, den Schutz „allen in [ihrem] Gebiet befindlichen und [ihrer] Herrschaftsgewalt unterstehenden Personen" gegenüber zu

---

[137] Siehe Deutscher Bundestag, Plenarprotokoll Nr. 1/167 v. 11.10.1951, S. 6852-6857. Siehe auch Deutscher Bundestag, Drucksache Nr. 1/2551 v. 11.9.1951.
[138] Siehe *Foschepoth*, (Fn. 130), S. 44.
[139] Siehe dazu oben Rn. 43.
[140] Siehe dazu oben Rn. 13-15.
[141] Internationaler Pakt über bürgerliche und politische Rechte (IPBPR) v. 19.12.1966 (BGBl. 1973 II S. 1534). Der IPBPR ist in Kraft für Deutschland seit 17.12.1973 sowie für alle Staaten der „Five Eyes": für Australien seit 13.8.1980, für Kanada seit 19.5.1976, für Neuseeland seit 28.12.1978, für das Vereinigte Königreich seit 20.5.1976 und für die Vereinigten Staaten von Amerika seit 8.6.1992.
[142] Siehe auch den weitgehend inhaltsgleichen Art. 12 der Allgemeinen Erklärung der Menschenrechte v. 10.12.1948. Bei der Erklärung handelt es sich um eine Resolution der VN-Generalversammlung, die als solche nicht bindend ist. Soweit der Erklärung heute völkergewohnheitsrechtliche Geltung zukommt, geht diese nicht über die Verbürgung des Art. 17 IPBPR hinaus.

gewährleisten.[143] Die gleiche Einschränkung des territorialen Anwendungsbereichs findet man in fast allen anderen hier einschlägigen Menschenrechtsverträgen.[144] Auch wenn man die Ansicht der Vereinigten Staaten von Amerika, dass den Rechten des Bürgerrechtspakts keine exterritoriale Wirkung zukommt,[145] nicht teilt, wird man nicht davon ausgehen können, dass Privatpersonen, die sich im Territorium der Bundesrepublik Deutschland aufhalten, der „Herrschaftsgewalt" der USA unterstehen. Voraussetzung hierfür wäre, dass sie der „Macht oder wirksamen Kontrolle" (*power or effective control*) der USA unterliegen.[146] Dies ist nur dann der Fall, wenn die betroffene Person der (physischen) Kontrolle durch einen Amtsträger des Staates unterworfen ist.[147] Eine rein „virtuelle Kontrolle" durch die Erfassung oder Überwachung der Daten einer Person ist hierfür nicht ausreichend.[148]

49. Darüber hinaus wäre die Frage der „Willkür" und der „Rechtswidrigkeit" des Eingriffs durch ausländische Geheimdienste in jedem Fall am Recht des Spionage treibenden Staates und nicht am deutschen Recht zu messen. Die NSA z.B. handelt nach US-amerikanischen Recht rechtmäßig, wenn sie Spionage im Ausland betreibt,[149] ebenso wie die Auslandsaufklärung des Bundesnachrichtendienstes nach Auffassung der Bundesregierung rechtmäßig ist und zum Beispiel nicht den datenschutzrechtlichen Anforderungen des Bundesdatenschutzgesetztes unterworfen ist.[150] Spione sind bei der heimlichen Informationsbeschaffung im Ausland grundsätzlich nicht an die Rechtsvorschriften ihres Heimatlandes gebunden. Es gilt: BND-Mitarbeiter sind an die *in Deutschland geltenden Gesetze* gebunden, aber nicht notwendigerweise an die *deutschen Gesetze*, wenn sie im Ausland tätig sind.[151]

---

[143] Siehe IPBPR, Art. 2 Abs. 1.

[144] Siehe z.B. EMRK, Art. 1; Übereinkommen über die Rechte des Kindes, Art. 2 Abs. 1; Internationales Übereinkommen zum Schutz der Rechte aller Wanderarbeitnehmer und ihrer Familienangehörigen, Art. 7.

[145] Zur Ansicht der USA siehe z.B. United States Department of State, Office of the Legal Adviser, Digest of United States Practice in International Law 2006, 2007, S. 346-349.

[146] *Human Rights Committee*, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add.13, 26.5.2004, S. 4, § 10.

[147] Siehe z.B. *Moeckli/Shah/Sivakumaran*, International Human Rights Law, 2. Aufl. 2014, S. 133.

[148] Zu den Fallgruppen, in denen die Ausübung von „Hoheitsgewalt" außerhalb des eigenen Staatsgebiets bejaht wurde, siehe *Kälin/Künzli*, Universeller Menschenrechtsschutz, 3. Aufl. 2013, S. 145-155.

[149] Siehe z.B. National Security Act of 1947, 50 USC Ch. 44; Executive Order 12333 of 4.12.1981: United States Intelligence Activities, as amended, https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf, und Presidential Policy Directive/PPD-28: Signals Intelligence Activities, 17.1.2014, https://fas.org/irp/offdocs/ppd/ppd-28.pdf. Siehe auch *Scott* (Fn. 75), S. 217, 220; *Wolf* (Fn. 128), S. 1040.

[150] Siehe § 1 Abs. 2 des Gesetzes über den Bundesnachrichtendienst (BND-Gesetz – BNDG) v. 20.12.1990 (BGBl. I S. 2954, 2979), zuletzt geändert durch Art. 7 des Gesetzes v. 20.6.2013 (BGBl. I S. 1602). Das Sammeln von Informationen durch den BND, einschließlich der heimlichen Beschaffung personenbezogener Daten, unterliegt nur dann dem Bundesdatenschutzgesetz, soweit sich das Sammeln der Informationen 'im Geltungsbereich dieses Gesetzes', d.h. im Bundesgebiet abspielt. Außerhalb Deutschlands ist der BND weitgehend frei von den Fesseln des deutschen Rechts.

[151] Vgl. z.B. Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) v. 26.6.2011 (BGBl. I S. 1254, 2298), zuletzt geändert durch Art. 2 Abs. 4 des Gesetzes v. 6.6.2013 (BGBl. I S. 1482). Soweit das Gesetz den BND ausdrücklich ermächtigt, die Telekommunikation zu überwachen und

50. Inwieweit die US-amerikanischen Rechtsvorschriften mit den Anforderungen des IPBPR an Gesetzmäßigkeit und Verhältnismäßigkeit vereinbar sind, wäre im Einzelfall zu prüfen. Für die Internet- und Telekommunikationsüberwachung durch die Geheimdienste fehlt es bislang an aussagekräftigen Entscheidungen des zur Überwachung der Einhaltung des IPBPR berufenen Menschenrechtsausschusses der Vereinten Nationen.[152] Insbesondere die Frage der Interessenabwägung zwischen Datenschutz und nationaler Sicherheit in Zeiten terroristischer Bedrohung ist international nicht abschließend geklärt. Zu berücksichtigen ist, dass den Staaten hier ein weiter Beurteilungsspielraum zukommt. Gerade im Hinblick auf die Praxis der Vereinigten Staaten von Amerika und anderer Staaten kann nicht davon ausgegangen werden, dass hier deutsche, sich aus dem Grundgesetz ergebende Maßstäbe zugrunde zu legen sind.[153]

51. Die Initiative Deutschlands und Brasiliens im Jahr 2013, das Recht auf Privatleben im Bürgerrechtspakt von 1966 durch eine Resolution der Generalversammlung der Vereinten Nationen für das digitale Zeitalter zu ergänzen und fortzuschreiben, um so die Privatsphäre des Einzelnen gegen geheimdienstliche Ausspähaktionen zu schützen,[154] dürfte vor diesem Hintergrund weitgehend ins Leere gehen. Die Vereinigten Staaten von Amerika sind zwar seit 1992 an den Pakt gebunden,[155] doch lassen sich neue völkerrechtliche Verpflichtungen nicht durch rechtlich unverbindliche Resolutionen der VN-Generalversammlung begründen. Die Bedeutung solcher Resolutionen besteht vor allem darin, dass sie als Bestandteil des völkerrechtlichen *„soft law“* langfristig zur Herausbildung von Völkergewohnheitsrecht beitragen können. Dies setzt aber voraus, dass sie konkrete Verpflichtungen statuieren und diese die Rechtsüberzeugung der Staaten widerspiegeln.

52. Ein Problem zeigt sich hier bereits bei der rechtswidrigen oder willkürlichen Sammlung personenbezogener Daten, die laut der Resolution das Recht auf Achtung der Privatsphäre verletzen können. Eine konkrete Verpflichtung scheitert hier bereits daran, dass zum Beispiel

---

aufzuzeichnen, betrifft dies nur Telekommunikationsanschlüsse im Inland oder Anschlüsse von deutschen Staatsangehörigen im Ausland; vgl. § 5 Abs. 2 G 10. Soweit der BND Anschlüsse von Ausländern im Ausland überwacht und deren Gespräche aufzeichnet, unterliegt er nicht dem G 10. Siehe auch *Schmahl* (Fn. 78), S. 221.

[152] Siehe die eher allgemein gehaltenen Aussagen des Menschenrechtsausschusses zu „National Security Agency Surveillance“ in *Human Rights Committee*, Concluding Observations on the Fourth Report of the United States of America; UN Doc. CCPR/C/USA/CO/4, 24.4.2014, S. 9-10 (§ 22).

[153] Vgl. *Margulies* (Fn. 46), S. 2152-2153, der davon ausgeht, dass die Aktivitäten der NSA mit Art. 17 IPBPR vereinbar sind.

[154] Siehe ‘Deutschland und Brasilien arbeiten an Resolution zu NSA’, Frankfurter Allgemeine Zeitung v. 28.10.2013, S. 2.

[155] Die USA sind seit 8.6.1992 an den Pakt gebunden; siehe United Nations, Multilateral Treaties Deposited with the Secretary-General, Chapter IV: Human Rights, http://treaties.un.org/.

bislang keine Einigkeit darüber besteht, ob es sich bei Internet Protocol (IP)-Adressen um „personenbezogene Daten" handelt.[156]

53. Auch reicht eine sachliche Ausdehnung des Schutzes der „Privatsphäre" auf den Online-Bereich allein nicht aus, um den begrenzten territorialen Anwendungsbereich des Paktes zu erweitern.[157] Dass sich aus der Resolution Nr. 68/167 der VN-Generalversammlung vom 18. Dezember 2013 keinerlei (neuen) rechtlichen Schranken für das exterritoriale Überwachen und Abfangen von Kommunikation, sowie die Sammlung personenbezogener Daten ergeben, zeigt sich bereits daran, dass diese im Konsensverfahren, d.h. ohne förmliche Abstimmung angenommen wurde, und sich weder die Vereinigten Staaten von Amerika noch andere in der Auslandsspionage aktive Staaten gezwungen sahen, eine formelle Abstimmung über die Resolution herbeizuführen und gegen diese zu stimmen.[158] Dies ist wenig verwunderlich, da sich die VN-Generalversammlung materiell darauf beschränkte, alle Staaten aufzufordern, „ihre Verfahren, Praktiken und Rechtsvorschriften hinsichtlich der Überwachung von Kommunikation, deren Abfangen und der Sammlung personenbezogener Daten zu überprüfen [...], mit dem Ziel, das Recht auf Privatheit zu wahren, indem sie die vollständige und wirksame Umsetzung aller ihrer Verpflichtungen nach den internationalen Menschenrechtsnormen sicherstellen".[159] Weiter ersuchte die Generalversammlung die Hohe Kommissarin der Vereinten Nationen für Menschenrechte, „einen Bericht über den Schutz und die Förderung des Rechts auf Privatheit im Kontext des innerstaatlichen und exterritorialen Überwachens und/oder Abfangens von digitaler Kommunikation und Sammelns personenbezogener Daten, namentlich in massivem Umfang, samt Auffassungen und Empfehlungen zur Prüfung durch die Mitgliedstaaten vorzulegen."[160] In diesem Ersuchen mag der bleibende praktische Wert der Resolution liegen, sollten sich die Staaten auf der Grundlage dieser Empfehlungen tatsächlich mit der Frage der Grundsätze, Standards und guten Praxis bei der Überwachung der digitalen Kommunikation und deren Auswirkungen auf das Recht der Privatsphäre befassen.

---

[156] Siehe z.B. *Inkster*, (Fn. 6), S. 53.

[157] Siehe in diesem Zusammenhang auch bereits die Resolution des VN-Menschenrechtsrates v. 19.6.2012, wonach dieselben Rechte, die die Menschen offline haben, auch online geschützt werden müssen; siehe UN Doc. A/HRC/20/L.13 (29.6.2012).

[158] Die VN-Generalversammlungsresolution Nr. 68/167 wurde am 18.12.2013 ohne Abstimmung angenommen; siehe UN Doc. A/68/PV.70 (18.12.2013), S. 20. Der Dritte Ausschuss der Generalversammlung hatte die Resolution bereits am 26.11.2013 ebenfalls ohne Abstimmung angenommen; siehe UN Doc. A/68/456/Add.2, 10.12.2013), S. 25 und UN Doc. GA/SHC/4094 (26.11.2013). Für die Position der Vereinigten Staaten im Dritten Ausschuss siehe United States Mission to the United Nations, 'Explanation of Position for the Third Committee Resolution on the Right To Privacy in the Digital Age by Ambassador Elizabeth Cousens, U.S. Representative to the UN Economic and Social Council', 26.11.2013, http://usun.state.gov/briefing/statements/218078.htm.

[159] VN-Generalversammlungsresolution Nr. 68/167, Abs. 4(c).

[160] Ebd., Abs. 5.

54. Auch in dieser Angelegenheit sollten jedoch keine zu großen Erwartungen geweckt werden, da sich Staaten wie die Vereinigten Staaten von Amerika nicht durch VN-Richtlinien in der Auslandsspionage einschränken lassen werden. Dies zeigt sich bereits daran, dass die Vereinigten Staaten von Amerika darauf hingewirkt haben, dass in der endgültigen Fassung der Resolution jeder Hinweis darauf, dass das exterritoriale Überwachen und/oder Abfangen von Kommunikation das Recht auf Privatsphäre verletzt, entfernt wurde. Hatte es im deutsch-brasilianischen Entwurf noch geheißen, dass die Generalversammlung tief besorgt sei „über die *Verletzungen und die Verstöße gegen die Menschenrechte*, die sich aus der Durchführung […] der exterritorialen Überwachung von Kommunikation, ihres Abfangens und der Sammlung personenbezogener Daten […] ergeben können“,[161] so heißt es in der endgültig angenommenen Resolution nur noch, dass die Generalversammlung tief besorgt sei, „über die *nachteiligen Auswirkungen*, die das [...] extraterritoriale[...] Überwachen[...] und/oder Abfangen[...] von Kommunikation, sowie die Sammlung personenbezogener Daten [...] *auf die Ausübung und den Genuss der Menschenrechte* haben können“.[162] Diese Änderung war für die Vereinigten Staaten wichtig, da diese der Auffassung sind, dass die Verpflichtungen aus dem Bürgerrechtspakt zum Schutz der Privatsphäre auf Ausländer außerhalb des US-Staatsgebiets keine Anwendung finden. Jede Verbindung zwischen exterritorialen Überwachungsmaßnahmen und dem Recht auf Privatsphäre galt es deshalb zu vermeiden. Daneben sollen nur die „rechtswidrige oder willkürliche“ Überwachungsmaßnahmen und das „rechtswidrige oder willkürliche“ Sammeln personenbezogener Daten das Recht auf Privatsphäre verletzen können.[163] Was rechtswidrig und willkürlich ist, ergibt sich jedoch aus dem nationalen Recht der jeweiligen Geheimdienste. Auch damit hatten die Vereinigten Staaten keine Probleme, da nach ihrer Auffassung die Spionagetätigkeit der NSA vom US-Recht gedeckt und sowohl von Gerichten als auch dem Kongress überwacht wird.[164]

55. Eine über die vertraglichen Verpflichtungen hinausgehende völkergewohnheitsrechtlich begründete Pflicht zur Achtung des Rechts auf Privatleben lässt sich nicht nachweisen.

---

[161] Siehe den zehnten Absatz der Erwägungsgründe des deutsch-brasilianischen Resolutionsentwurfs, UN Doc. A/C.3/68/L.45 (7.11.2013).
[162] VN-Generalversammlungsresolution Nr. 68/167, Erwägungsgründe, Abs. 10.
[163] Zur US-amerikanischen Strategie den Resolutionstext zu ‘verwässern’ siehe die Verhandlungsanweisungen an die amerikanische VN-Delegation ‘Right to Privacy in the Digital Age – U.S. Redlines’, abgedruckt bei *Lynch*, ‘Exclusive: Inside America’s Plan to Kill Online Privacy Rights Everywhere’, Foreign Policy, 20 November 2013, http://thecable.foreignpolicy.com/. Siehe auch *MacAskill/Ball*, ‘UN surveillance resolution goes ahead despite attempts to dilute language’, The Guardian, 21.11.2013, http://www.theguardian.com/.
[164] Siehe *Margulies* (Fn. 46), S. 2152.

III. Abkommen über Erhebung, Speicherung und Austausch von Daten

56. *Leitfrage: Könnten Abkommen Deutschlands mit einem oder mehreren Staaten der sog. „Five Eyes" Erhebung, Speicherung auf Vorrat und Austausch von Daten legitimieren? Gibt oder gab es solche Abkommen und wenn ja mit welchen Staaten und mit welchem Inhalt?*

1. Das sog. „No Spy-Abkommen" der sog. „Five Eyes"-Staaten

57. Als Konsequenz aus der NSA-Affäre wurde in Deutschland der Abschluss eines sog. „No Spy-Abkommens" mit den USA gefordert. Bereits am 13. August 2013 kündigte der für die Geheimdienste zuständige damalige Kanzleramtschef Pofalla ein solches Abkommen mit den USA an. Die USA hätten den Abschluss eines solchen Abkommens angeboten.[165] Nach Aussage des stellvertretenden Regierungssprechers vom 25. Oktober 2013 erwartete die Bundesregierung bis zum Ende des Jahres 2013 „von den USA den Abschluss eines Abkommens, in dem die Tätigkeit und die Zusammenarbeit der Nachrichtendienste geregelt und festgelegt werden. Dazu gehört u. a., dass wir uns gegenseitig nicht ausspionieren".[166]

58. In diesem Zusammenhang wurde und wird immer wieder auch auf die britisch-amerikanische Fernmeldeaufklärungsvereinbarung vom 5. März 1946 verwiesen, der später auch Australien, Kanada und Neuseeland beigetreten sind. Diese sog. „Five Eyes" sollen angeblich übereingekommen sein, sich nicht gegenseitig auszuspähen. Bei dieser heute auf der Internetseite der NSA veröffentlichten „Vereinbarung" scheint es sich jedoch eher um eine politische Abmachung – ein sog. „Gentlemen's Agreement" oder ein „Memorandum of Understanding" – zwischen den Geheimdiensten als um einen völkerrechtlich verbindlichen Vertrag zwischen den Staaten zu handeln.[167] Ein Ausspähverbot wird nicht ausdrücklich erwähnt; vielmehr geht es um den umfassenden Austausch von Geheimdienstinformationen, der ein gegenseitiges Ausspähen wohl überflüssig macht.

59. Bislang haben die Vereinigten Staaten von Amerika noch mit keinem anderen Staat ein rechtsverbindliches „No Spy"-Abkommen geschlossen. Am 11. Februar 2014 erwiderte US-Präsident Obama in einer gemeinsamen Pressekonferenz mit dem französischen Präsidenten Hollande auf die Frage, ob er das „No Spy"-Abkommen mit England nicht auf Frankreich ausdehnen wolle: „Es gibt kein Land, mit dem wir ein No Spy-Abkommen haben. Wir haben, wie jedes andere Land auch, Geheimdienstfähigkeiten, und dann haben wir eine Reihe von

---

[165] Siehe 'Deutsch-amerikanisches Anti-Spionage-Abkommen geplant', Reuters Deutschland, 12.8.2013, http://de.reuters.com/.

[166] Siehe Bundesregierung, 'Regierungspressekonferenz v. 25.10.2013', http://www.bundesregierung.de/.

Partnerschaften mit allen Arten von Ländern."[168] Auch andere Staaten scheinen solche Abkommen bislang nicht eingegangen zu sein. Dies bedeutet nicht, dass solche Abkommen völkerrechtlich nicht möglich wären.

60. Es stellt sich jedoch die Frage, ob der Tatbestand der Spionage, anders als die Behandlung gefasster Spione, im Hinblick auf die nationalen Sicherheitsinteressen der Staaten einer völkervertraglichen Verbotsregelung überhaupt sinnvoll zugänglich ist. Ein solches Verbot stünde wohl von Anfang an unter dem Vorbehalt des Schutzes „nationaler Interessen", des Rechts zur Selbstverteidigung, des Notstandes, der Notlage, einer grundlegenden Änderung der Umstände oder anderer möglicher Rechtfertigungen des Vertragsbruchs. In jedem Fall käme es darauf an, ob durch ein solches Abkommen mit den Vereinigten Staaten lediglich das Ausspähen deutscher Regierungsstellen und Behörden sowie der deutschen Wirtschaft oder jegliche Spionagetätigkeit in Deutschland ausgeschlossen werden soll. Letzteres erscheint im Hinblick auf eventuell von deutschem Boden ausgehende Terrorgefahren unwahrscheinlich. Man wird sich in den Vereinigten Staaten daran erinnern, dass einige der Attentäter vom 11. September 2001 in Hamburg studiert hatten.[169] Vor diesem Hintergrund wurde von Anfang an darauf hingewiesen, dass man sich keine zu großen Hoffnungen auf den Abschluss eines völkerrechtlich verbindlichen „No Spy"-Abkommens machen sollte. Wenn überhaupt, hätte die Obama-Regierung zu einer politischen Abmachung bereit sein dürfen, die den Staaten normalerweise größere Handlungsspielräume bei deren „Nichterfüllung" lässt. Aber auch eine solche offizielle förmliche politische Vereinbarung mit Deutschland erschien von Beginn an als eher unwahrscheinlich. Die USA hätten eine solche nicht eingehen können, ohne dass andere Partner und Verbündete den Abschluss ähnlicher Abkommen gefordert hätten. Auch hätte jede auch rechtlich unverbindliche Vereinbarung den politischen Preis erhöht, den zukünftige US-Regierungen für Spionagetätigkeiten in Deutschland zu zahlen gehabt hätten.[170] Trotz dieser Bedenken hielt die Bundesregierung zunächst am Abschluss eines „No Spy"-

---

[167] Der Text des British-U.S. Communication Intelligence Agreement v. 5.3.1946, findet sich auf der Webseite der NSA unter http://www.nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf.

[168] The White House, 'Press Conference by President Obama and President Hollande of France', 11.2.2014, http://www.whitehouse.gov/ (Übersetzung des Autors). Siehe auch 'Treffen mit Hollande: Obama erteilt No-Spy-Abkommen klare Absage', SpiegelOnline, 11.2.2014, http://www.spiegel.de/.

[169] Siehe 'Mutmaßliche Terroristen haben in Hamburg studiert', Frankfurter Allgemeine Zeitung v. 15.09.2001, S. 8.

[170] Siehe z.B. *Talmon*, 'Ich spioniere, du spionierst, alle spionieren – und es ist erlaubt', Frankfurter Allgemeine Zeitung v. 1.11.2013, S. 7. Kritisch gegenüber der Praktikabilität eines "No Spy-Abkommens" auch *Schmahl* (Fn. 78), S. 22 und ebenso bereits *Chesterman*, 'Secret Intelligence', in: Wolfrum (ed.), Max Planck Encyclopedia of Public International Law, vol. IX, 2012, S. 66-72 (66); *Doehring*, 'Spionage im Friedensvölkerrecht', in: Bundesamt für Verfassungsschutz (Hrsg.), Verfassungsschutz in der Demokratie, 1990, S. 307-324 (309: „ebenso merkwürdig wäre eine Vereinbarung, daß gegenseitige Spionage verboten sei").

Abkommens fest.[171] Noch am 15. Januar 2014 ließ die Bundesregierung in einer Debatte des Deutschen Bundestages zu den Verhandlungen über ein „No Spy"-Abkommen erklären, dass „die Verhandlungen mit den Amerikanern über eine verbindliche Vereinbarung zu nachrichtendienstlichen Tätigkeiten weitergeführt werden, und deshalb – da kann die Opposition ganz beruhigt sein – werden sie auch weitergeführt."[172] Nur wenige Wochen später schien jedoch selbst die Bundesregierung erkannt zu haben, dass es ein „No Spy"-Abkommen mit den Vereinigten Staaten nicht geben wird.[173] Am 27. Februar 2014 musste Außenminister Steinmeier bei einem Besuch in Washington einräumen, dass es bei unterschiedlichen Bewertungen der Bedeutung von Sicherheit, Freiheit und Privatsphäre keinen Sinn macht, „Verhandlungen über ein bilaterales ‚No-Spy'-Abkommen zu beginnen". Stattdessen soll über „die Tatsache gesprochen werden, dass wir uns in diesen Fragen nicht immer einig sind. […] Unsere Argumente werden von der anderen Seite nicht immer geteilt, aber es gibt Punkte, bei denen wir vielleicht niemals 100 Prozent übereinstimmen."[174] Statt eines Abkommens setzt Deutschland jetzt auf einen „Cyberdialog" zwischen den Regierungen, der Wissenschaft und der Zivilgesellschaft beider Länder, um Unterschiede und Gemeinsamkeiten im Umgang mit dem Schutz der Privatsphäre zu definieren[175] – ein diplomatisches Begräbnis erster Klasse der von Anfang an realitätsfernen deutschen Hoffnungen auf ein „No Spy"-Abkommen.

2. Rechtswirkungen sog. „No Spy-Abkommen"

61. Bei entsprechendem politischen Willen könnte die Bundesrepublik Deutschland in einem sog. „No Spy-Abkommen" mit anderen Staaten die Erhebung, Speicherung auf Vorrat und den Austausch von Daten zwischen den Geheimdiensten völkerrechtlich verbindlich regeln. Im Völkerrecht gilt grundsätzlich Vertragsfreiheit. Ein solcher Vertrag wäre mangels eines Verstoßes gegen eine einschlägige Norm des zwingenden Völkerrechts, von der nicht

---

[171] Siehe 'No-Spy-Abkommen: Chronologie eines Missverständnisses', Süddeutsche Zeitung Online, 14.1.2014, http://www.sueddeutsche.de/.

[172] Siehe die Erklärung des Parlamentarischen Staatssekretärs beim Bundesminister der Innern, Dr. Günter Krings, in der Aktuellen Stunde zur 'Haltung der Bundesregierung zu den Verhandlungen über ein No-Spy-Abkommen zwischen den USA und der Bundesrepublik Deutschland', Deutscher Bundestag, Plenarprotokoll Nr. 18/7 v. 15.1.2014, S. 366 (B). Siehe auch die Erklärung des Koordinators der Bundesregierung für die transatlantischen Beziehungen, Philipp Mißfelder, vom selben Tag: 'Der Abschluss eines No-Spy-Abkommens mit den Vereinigten Staaten ist für Deutschland wichtig, um die Vertrauensbasis mit unseren Freunden in den USA wiederherzustellen. […] Berichten, wonach die Verhandlungen zum No-Spy-Abkommen schon jetzt gescheitert wären, müssen wir deutlich widersprechen. Im Gegenteil: Es wird weiter verhandelt'; siehe 'Mißfelder: Scheitern des No-Spy-Abkommens wäre Rückschlag in den Beziehungen zu den USA', 15.1.2014, http://www.presseportal.de/.

[173] Siehe 'Germany gives up on no-spy deal with US', Financial Times, 13.2.2014, http://ft.com/.

[174] U.S. Department of State, 'Remarks with German Foreign Minister Frank-Walter Steinmeier After Their Working Lunch', 27.2.2014, http://www.state.gov/ (Übersetzung des Autors).

abgewichen darf (*jus cogens*), nicht von vorneherein nichtig.[176] Insbesondere kann nicht davon ausgegangen werden, dass das Rechts auf Achtung des Privatlebens *jus cogens*-Status erlangt hat.[177] Dies zeigt sich u.a. daran, dass vom Recht auf Achtung des Privat- und Familienlebens im Notstandsfall abgewichen werden darf.[178]

62. Der Abschluss eines völkerrechtlichen Vertrages über die nachrichtendienstliche Zusammenarbeit kann die Vertragsparteien aber grundsätzlich nicht von anderweitig bestehenden völkerrechtlichen oder verfassungsrechtlichen Pflichten befreien. Bestehende entgegenstehende völkervertragliche Verpflichtungen (z.B. im Menschenrechtsbereich) können nur durch spätere Verträge zwischen denselben Vertragsparteien oder durch neu entstehendes Völkergewohnheitsrecht abbedungen werden.[179] Bestehende grundrechtliche Verpflichtungen können durch den Abschluss eines völkerrechtlichen Vertrages nicht ausgehebelt werden. Soweit ein solches Abkommen gegen Grundrechte verstieße, wäre es zwar völkerrechtlich bindend (da sich ein Staat auf internationaler Ebene grundsätzlich nicht auf sein nationales Recht berufen kann),[180] dürfte aber von deutschen Staatsorganen nicht ausgeführt werden. Die Nichterfüllung des Vertrags (auch aus Gründen des Grundrechtsschutzes) hätte die völkerrechtliche Verantwortlichkeit der Bundesrepublik Deutschland wegen Vertragsbruchs zur Folge.[181]

---

[175] Auswärtiges Amt, 'Außenminister Steinmeier in Washington', 1.3.2014, http://www.auswaertiges-amt.de/.
[176] Siehe Wiener Übereinkommen über das Recht der Verträge (WÜRV) v. 23.5.1969 (BGBl. 1985 II S. 927), Art. 53.
[177] Das Recht auf Privatleben findet sich z.B. nicht in der Liste der Beispiele für *jus cogens*, die die Völkerrechtskommission der Vereinten Nationen im Jahr 2006 aufgestellt hat; siehe *International Law Commission*, Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, UN Doc. A/CN.4/L.702, 18.7.2006, S. 21 (§ 33). Contra *Orakhelashvili*, Peremptory Norms in International Law, 2006, S. 60, der auch das Recht auf „Familien- und Privatleben" als *jus cogens* ansieht.
[178] Siehe z.B. EMRK, Art. 15 Abs. 2; IPBPR, Art. 4 Abs. 2. Zur Abweichung im Notstandsfall als Kriterium für die Feststellung von Normen des *jus cogens*, vgl. *Orakhelashvili* (Fn. 177), S. 56-58.
[179] Siehe WÜRV, Art. 30.
[180] WÜRV, Art. 27, 46.
[181] Vgl. *International Law Commission*, Articles on Responsibility of States for Internationally Wrongful Acts, 31.5.2011; UN Doc. A/RES/56/83 v. 12.12.2001, Annex, Art. 1.

IV. Individueller Rechtsschutz gegen Maßnahmen der sog. „Five Eyes“

63. Leitfrage: Welche Möglichkeiten eines individuellen Rechtsschutzes haben Betroffene bei der Erhebung, Speicherung auf Vorrat und Weitergabe ihrer Daten aus und über Telekommunikationsvorgänge und Internetnutzung durch Staaten der sog. „five eyes“ vor internationalen Gremien (EGMR, UN Menschenrechtsausschuss etc.)?

1. Individualbeschwerde vor dem Europäischen Menschenrechtsgerichtshof

64. Nach Artikel 34 EMRK kann jede natürliche Person, nichtstaatliche Organisation (z.B. Wirtschaftsunternehmen oder NGOs) oder Personengruppe, die behauptet, durch eine der Vertragsparteien in ihren Rechten aus der Konvention oder den Zusatzprotokollen verletzt worden zu sein, den Europäischen Gerichtshof für Menschenrechte (EGMR) mit einer Beschwerde befasst werden (sog. „Individualbeschwerde“).

65. Eine Individualbeschwerde ist nur gegen Vertragsparteien der EMRK zulässig, d.h. im vorliegenden Fall gegen das Vereinigte Königreich.[182] Die übrigen Staaten der sog. „Five Eyes“-Allianz sind nicht an die EMRK gebunden. Daneben ist aber auch an eine Beschwerde gegen die Bundesrepublik Deutschland zu denken, wenn diese gegen das Recht auf Achtung des Privatlebens (z.B. durch Anforderung, Entgegennahme und Auswertung von persönlichen Daten von Personen im Bundesgebiet, die von den Nachrichtendiensten der sog. „Five Eyes“ erhoben wurden) verstößt, eine sich aus der EMRK ergebende Pflicht zum Schutz der Bewohner des Bundesgebiets gegen ausländische Überwachungsmaßnahmen verletzt oder wenn diese sich anderweitig an einer rechtswidrigen Erhebung, Speicherung oder Auswertung von Daten durch ausländische Nachrichtendienste beteiligt.

66. Zulässigkeitsvoraussetzung für die Beschwerde ist die Erschöpfung aller innerstaatlichen Rechtsbehelfe gegen die Überwachungsmaßnahmen.[183] Zu ergreifen sind nicht nur gerichtliche, sondern grundsätzlich sämtliche (auch verwaltungsbehördliche) Rechtsbehelfe, die eine verbindliche Entscheidung zur Folge haben. Bei der Prüfung, ob der Rechtsweg erschöpft wurde, sind stets die besonderen Umstände des Einzelfalls zu berücksichtigen. Nicht wirksame oder von vornherein aussichtslose Rechtsbehelfe müssen grundsätzlich nicht

---

[182] Die EMRK ist für das Vereinigte Königreich seit 3.9.1953 in Kraft. Ein erstes durch die Enthüllungen von Edward Snowden angestoßenes Verfahren wurde am 4.9.2013 gegen das Vereinigte Königreich angestrengt; siehe ECtHR (Fourth Section), *Big Brother Watch and Others v. United Kingdom*, Application No. 58170/13, http://hudoc.echr.coe.int/. Beschwerdeführerin ist u.a. die Deutsche Dr. Constanze Kurz aus Berlin, die sich durch die Überwachungsmaßnahmen des britischen Nachrichtendienstes GCHQ und anderer britischer Dienste in ihrem Recht auf Achtung des Privatlebens verletzt sieht.

[183] EMRK, Art. 35 Abs. 1.

ergriffen werden.[184] Sofern Rechtsbehelfe gegen nachrichtendienstliche Überwachungsmaßnahmen bestehen, kann nicht ohne weiteres davon ausgegangen werden, dass diese unwirksam oder von vornherein aussichtslos sind.[185]

67. Nach Artikel 34 EMRK muss der Beschwerdeführer behaupten, in einem seiner Rechte aus der EMRK verletzt zu sein, d.h. er muss persönlich *betroffen* und *beschwert* sein. Klagen *in abstracto* gegen bestehende Gesetze oder Maßnahmen sind grundsätzlich unzulässig.[186] Bei Beschwerden gegen gesetzliche Bestimmungen begründet grundsätzlich erst der Vollzugsakt die Betroffenheit des Beschwerdeführers. Eine Ausnahme besteht bei Beschwerden gegen geheime Überwachungsmaßnahmen oder Gesetze, die geheime Überwachungsmaßnahmen ermöglichen. In diesem Fall muss der Beschwerdeführer im Interesse eines effektiven Rechtsschutzes nicht behaupten, dass er selbst Opfer der Maßnahme wurde, da ihm dies infolge des geheimen Charakters der Maßnahme meist nicht bekannt sein dürfte. In einem solchen Fall soll es ausreichen, dass der Beschwerdeführer geltend macht, allein durch die Existenz des Gesetzes oder die Existenz bestimmter Maßnahmen in seinen Rechten betroffen zu sein. Er kann somit z.B. überprüfen lassen, ob ein Gesetz, das Maßnahmen zur Überwachung von Telekommunikationsvorgängen ermöglicht, den Anforderungen an die Einschränkung des Rechts auf Achtung des Privatlebens genügt.[187] Das Gericht ermittelt die Opfereigenschaft des Beschwerdeführers dann unter Berücksichtigung der behaupteten Rechtsverletzung, des geheimen Charakters der in Frage stehenden Maßnahmen und der Verbindung zwischen dem Beschwerdeführer und diesen Maßnahmen.[188]

68. Die Erleichterung des Nachweises der Opfereigenschaft des Beschwerdeführers bei geheimen Überwachungsmaßnahmen erfährt jedoch dann eine Einschränkung, wenn sich der Beschwerdeführer nicht gegen ein bestehendes Überwachungsgesetz, sondern gegen *tatsächliche* Überwachungsmaßnahmen wendet. Nicht jedermann, der „befürchtet", Opfer von Überwachungsmaßnahmen geworden zu sein, ist beschwerdebefugt. Erforderlich ist vielmehr eine „begründete Wahrscheinlichkeit" (*reasonable likelihood*), dass die Maßnahmen auf den Beschwerdeführer angewandt wurden.[189] Es ist somit nach der ständigen

---

[184] Siehe *Grabenwarter/Pabel* (Fn. 29), § 13, Rn. 23, 30.
[185] Vgl. das „Statement of Facts" in ECtHR (Fourth Section), *Big Brother Watch and Others v. United Kingdom*, Application No. 58170/13, http://hudoc.echr.coe.int/. Siehe auch Bundesverwaltungsgericht, Pressemitteilung Nr. 35/2014 v. 28.5.2014 zur Klage gegen strategische Telekommunikationsüberwachung durch den BND im Jahr 2010, http://www.bverwg.de/.
[186] St. Rspr., siehe z.B. ECtHR (Fourth Section), *Kennedy v. United Kingdom*, Application No. 26839/05, Judgment, 18.5.2010, § 119.
[187] Zu den Voraussetzungen für die Einschränkung des Rechts auf Achtung des Privatlebens, siehe oben Rn. 17-20.
[188] Siehe ECtHR (Plenary), *Klass and Others v. Germany*, Application No. 5029/71, Judgment, 6.9.1978, § 34.
[189] Siehe ECtHR (Fourth Section), *Kennedy v. United Kingdom*, Application No. 26839/05, Judgment, 18.5.2010, § 122.

Rechtsprechung des EGMR bei der Opfereigenschaft zwischen allgemeinen Beschwerden gegen Überwachungsgesetze und eine Praxis geheimer Überwachung (potentielle Betroffenheit ausreichend) und Beschwerden gegen konkrete Überwachungsmaßnahmen (begründete Wahrscheinlichkeit der Betroffenheit erforderlich) zu unterscheiden.[190]

69. Bei Beschwerden gegen Überwachungsgesetze oder eine Praxis geheimer Überwachung hat der EGMR die Anforderungen an die Betroffenheit des Beschwerdeführers weiter gelockert, wenn es auf nationaler Ebene keine Möglichkeit gibt, die angebliche Anwendung geheimer Überwachungsmaßnahmen überprüfen zu lassen. In einem solchen Fall, in dem man nicht sagen kann, dass weit verbreitetes Misstrauen und Sorge in der Bevölkerung über den Missbrauch geheimer Überwachungsbefugnisse unberechtigt sind, besteht eine größere Notwendigkeit für eine Überprüfung durch den Gerichtshof, auch wenn das tatsächliche Risiko der Überwachung gering ist.[191]

70. Bei der Individualbeschwerde zum EGMR handelt es sich um eine der effektivsten, wenn nicht die effektivste Rechtsschutzmöglichkeit des Einzelnen im Menschenrechtsbereich auf internationaler Ebene. Die Urteile des Gerichtshofs sind für die Vertragsstaaten bindend.[192] Diese müssen alle erforderlichen Maßnahmen (einschließlich Änderung ihrer Gesetzgebung) treffen, um Verletzungen der EMRK abzustellen und um sicherzustellen, dass sich diese nicht wiederholen. Die Überwachung der Durchführung sowie die Durchsetzung der Urteile des Gerichtshofs obliegen dem Ministerkomitee des Europarats.[193]

2. Individualbeschwerde vor dem Menschenrechtsausschuss der Vereinten Nationen

71. Nach Artikel 2 des Fakultativprotokolls zum IPBPR[194] können Einzelpersonen (also nicht – anders als bei der EMRK – juristische Personen wie NGOs oder Wirtschaftsunternehmen), die behaupten in einem ihrer im IPBPR niedergelegten Rechte verletzt zu sein, dem Menschenrechtsausschuss der Vereinten Nationen eine schriftliche Mitteilung über die Rechtsverletzung zur Prüfung einreichen. Der Ausschuss nimmt jedoch nur Mitteilungen gegen Vertragsstaaten des Fakultativprotokolls entgegen. Das Vereinigte Königreich und die Vereinigten Staaten von Amerika sind – anders als die Bundesrepublik Deutschland,

---

[190] Ebd., § 123.
[191] Ebd., § 124; ECtHR (Fourth Section), *Hadzhiev v. Bulgaria*, Application No. 22373/04, Judgment, 23.10.2012, § 39.
[192] EMRK, Art. 46 Abs. 1.
[193] EMRK, Art. 46 Abs. 2.
[194] Fakultativprotokoll zum Internationalen Pakt über bürgerliche und politische Rechte v. 19.12.1966 (BGBl. 1992 II S. 1247).

Australien, Kanada und Neuseeland – nicht Vertragsparteien des Protokolls, so dass eine Individualbeschwerde gegen diese beiden Staaten nicht möglich ist.

72. Der Menschenrechtsausschuss prüft die Rechtsverletzung in einem gerichtsähnlichen Verfahren und teilt seine „Auffassung" dem betroffenen Vertragsstaat und der Einzelperson mit.[195] Diese „Auffassungen" sind für die betroffenen Vertragsstaaten rechtlich nicht bindend,[196] entfalten aber aufgrund ihrer Veröffentlichung im Jahresbericht des Ausschusses an die Generalversammlung der Vereinten Nationen und aufgrund der Stellung und des Ansehens des Ausschusses „großes [politisches und moralisches] Gewicht".[197]

3. Individualbeschwerde vor der Interamerikanischen Menschenrechtskommission

73. Die Amerikanische Menschenrechtskonvention (AMRK) sieht ebenso wie die EMRK die Möglichkeit einer Individualbeschwerde wegen Verletzungen der Rechte aus der AMRK vor.[198] Diese ist jedoch nur gegen Vertragsparteien der AMRK möglich. Die beiden nordamerikanischen Mitglieder der „Five Eyes", die Vereinigten Staaten von Amerika und Kanada, sind jedoch nicht Parteien der AMRK, so dass eine Individualbeschwerde wegen Verletzung von Rechten aus der AMRK ausscheidet. Die beiden Staaten sind aber Mitglieder der Organisation Amerikanischer Staaten (OAS). Nach Artikel 20 (b) des Statuts der Interamerikanischen Menschenrechtskommission kann gegen OAS-Mitgliedstaaten, die nicht Vertragsparteien der AMRK sind, Individualbeschwerde wegen Verletzung der in der Amerikanischen Deklaration der Rechte und Pflichten der Menschen erwähnten Rechte erhoben werden.[199] Die Amerikanische Menschenrechtsdeklaration[200] erwähnt in Artikel V das Recht auf Privatleben und in Artikel X das Recht auf Unverletzlichkeit des Schriftverkehrs, worunter sich auch der Schutz persönlicher Daten subsumieren lässt.

74. Die Interamerikanische Menschenrechtskommission untersucht die Rechtsverletzung und trifft eine „Empfehlung" in der Sache, der aber keine Rechtsverbindlichkeit zukommt. Ebenso wie der Menschenrechtsausschuss der Vereinten Nationen werden die Empfehlungen in der Regel im Jahresbericht der Kommission an die Generalversammlung der OAS veröffentlicht.

---

[195] Ebd., Art. 5 Abs. 1 und 4.
[196] Siehe *Kälin/Künzli* (Fn. 148), Rn. 647.
[197] International Court of Justice, *Ahmadou Sadio Diallo (Republic of Guinea v. Democratic Republic of Congo)*, Merits, Judgment, ICJ Reports 2010, S. 639, 664 (§ 66).
[198] AMRK, Art. 44.
[199] Organisation of American States, Statute of the Inter-American Commission on Human Rights, October 1979, http://www.cidh.org/basicos/english/Basic17.Statute%20of%20the%20Commission.htm.
[200] Amerikanische Deklaration der Rechte und Pflichten der Menschen, 1948, abgedruckt in *Brownlie/Goodwin-Gill* (ed.), Basic Documents on Human Rights, 5. Aufl. 2006, S. 927.

Der Wirksamkeit der Empfehlungen, insbesondere gegenüber den Vereinigten Staaten von Amerika sind enge Grenzen gesetzt.[201]

[201] Siehe *Buergenthal/Thürer* (Fn. 70), S. 307.