HUMBOLDT-UNIVERSITÄT ZU BERLIN

HU Berlin | Juristische Fakultät | Prof. Dr. G. Nolte | 10099 Berlin

Deutscher Bundestag
1. Untersuchungsausschuss der 18. Wahlperiode
Der Vorsitzende – Herrn Prof. Dr. Patrick Sensburg, MdB
Platz der Republik 1
11011 Berlin

- vorab per E-Mail

Deutscher Bundestag
1. Untersuchungsausschuss
der 18. Wahlperiode

MAT A SV-4/1

zu A-Drs.: 56

Deutscher Bundestag
1. Untersuchungsausschuss
28. Mai 2014

Sehr geehrter Herr Vorsitzender,

ich darf Ihnen hiermit die schriftliche Zusammenfassung meiner Stellungnahme für die Anhörung am 5. Juni übermitteln.

Mit freundlichen Grüßen

(Unterschrift)

Dr. Helmut Philipp Aust

Juristische Fakultät

Öffentliches Recht,
Völker- und Europarecht

Dr. Helmut Philipp Aust

Datum:
27. Mai 2014

Bearbeiter/in:

Postanschrift:
Humboldt-Universität zu Berlin
Unter den Linden 6
10099 Berlin
Telefon +49 [30] 2093-3357
Telefax +49 [30] 2093-3384

helmut.aust@jura.hu-berlin.de
http://nolte.jura.hu-berlin.de/staff/ha

Sitz:
Unter den Linden 9
Raum 119
10117 Berlin

Verkehrsverbindungen:
S- und U-Bahnhof Friedrichstraße
Bus: Linien 100, 200 und TXL,
Haltestelle Staatsoper

1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages

Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014

Dr. Helmut Philipp Aust, Humboldt-Universität zu Berlin*

A. Einleitung

1. Ich wurde beauftragt, für den 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages ein Sachverständigengutachten über völker- und europarechtliche Fragen der Erhebung, Speicherung und Verarbeitung von Daten zu erstatten. Im Zusammenhang mit dem Untersuchungsauftrag des Ausschusses stellen sich insbesondere Fragen im Hinblick auf Überwachungsmaßnahmen durch Nachrichtendienste der sog. „five eyes“-Staaten (Vereinigte Staaten von Amerika, Vereinigtes Königreich, Australien, Kanada, Neuseeland).

* Wissenschaftlicher Mitarbeiter und Habilitand am Lehrstuhl für Öffentliches Recht, Völkerrecht und Europarecht der Juristischen Fakultät der Humboldt-Universität zu Berlin.

2. Bei der Beantwortung der einzelnen übermittelten Fragen ist zu berücksichtigen, dass im Zuge der durch Edward Snowden angestoßenen Enthüllungen eine Vielzahl an unterschiedlichen Überwachungsmaßnahmen im Raum steht. Diese werfen naturgemäß auch unterschiedliche rechtliche Fragen auf. Wenn ein Staat Privatunternehmen der Internetbranche, die in seinem Staatsgebiet ansässig sind, zur Herausgabe von Daten anhält – wie es im Rahmen des NSA-Programms PRISM[1] geschehen sein soll – stellen sich andere Rechtsfragen als bei der Anzapfung eines transatlantischen Glasfaserkabels, wie es vom britischen Geheimdienst GCHQ im Rahmen des Tempora-Programms unternommen worden sein soll. Wieder andere Rechtsprobleme werden aufgeworfen, wenn mit diplomatischer Immunität ausgestatte Mitarbeiter eines ausländischen Nachrichtendienstes Gespräche im Umfeld eines Botschaftsgeländes abhören, wie es im Hinblick auf die Ausspähung der Handykommunikation der Bundeskanzlerin berichtet wurde.

3. Nach den übermittelten Leitfragen für die Sachverständigengutachten soll, wo erforderlich, auch danach differenziert werden, ob Daten aus und zu innerdeutschen Verbindungen, Verbindungen von und nach Deutschland und Verbindungen im Ausland betroffen sind. Diese Unterscheidungen können aufgrund von technischen Gegebenheiten in der Praxis vielfach nicht klar identifiziert werden. Die „Wege", die z.B. eine E-Mail zwischen zwei deutschen Internetnutzern mit deutschen Accounts, die sich auf deutschem Staatsgebiet aufhalten, zurücklegt, sind nur schwer bis gar nicht nachvollziehbar.[2] Vielfach werden auch rein innerstaatliche Kommunikationsvorgänge über ausländische Netze geleitet werden. Durch diese Unsicherheit verliert eine strikte Unterscheidung zwischen Inlands- und Auslandsüberwachung teilweise ihren Sinn – was auch eine treibende Kraft für die Diskussion um die Überwachungspraxis der NSA in den Vereinigten Staaten darstellt.[3] Dies soll nicht bedeuten, dass es nicht technisch möglich wäre, eine Internetinfrastruktur zu schaffen, in der sich diese Probleme der Lokalisierbarkeit von Datenwegen so nicht mehr stellen würden. Damit einhergehen würde aber vermutlich eine erhebliche Veränderung des Charakters des Internets als globales und grundsätzlich offenes Kommunikationsforum. Nicht umsonst haben bisher vor allem autoritäre Staaten über die Schaffung von eigenen internetähnlichen Strukturen nachgedacht.[4]

4. Die Affäre um das Ausmaß der Überwachungsmaßnahmen von NSA, GCHQ und anderen Diensten ist letztlich eine Konsequenz der veränderten geopolitischen Lage. Spionage wurde klassischerweise nicht als menschenrechtliches Problem aufgefasst. Solange sich nachrichtendienstliche Tätigkeiten vor allem auf den staatlichen Apparat des „Gegners" bezogen haben, wurde dies unter rechtsstaatlichen Gesichtspunkten als nicht weiter bedrohlich wahrgenommen. Die nach dem Ende des Kalten Krieges veränderte weltpolitische Lage, in der Bedrohungen durch nicht-staatliche Akteure im Mittelpunkt der Aufmerksamkeit standen, führte zu der enormen Ausdehnung nachrichtendienstlicher

---

[1] Die Rechtsgrundlage für dieses Programm ist in Sec. 702 des Foreign Intelligence Surveillance Act vom 25.10.1978 zu erblicken, Publ. L 95-511, 92 Stat. 1783, p. 1566.

[2] Dazu auch Christopher Kuner, *Transborder Data Flows and Data Privacy Laws*, Oxford 2013, S. 6 f.

[3] Daniel Byman/Benjamin Wittes, Reforming the NSA – How to Spy After Snowden, *Foreign Affairs*, May/June 2014, abrufbar unter http://www.foreignaffairs.com/articles/141215/daniel-byman-and-benjamin-wittes/reforming-the-nsa (zuletzt aufgerufen am 23.5.2014).

[4] Zur Einschränkung globaler Datenströme durch vornehmlich autoritäre Regime siehe Kuner (Fn. 2), S. 30 f.; sowie Matthias C. Kettemann, Das Internet als internationales Schutzgut: Entwicklungsperspektiven des Internetvölkerrechts anlässlich des Arabischen Frühlings, *ZaöRV* 72 (2012), S. 469-482.

Überwachungsmaßnahmen. Die Suche nach der berühmten „Nadel im Heuhaufen" führt zu einer Erfassung des Kommunikationsverhaltens breiter Bevölkerungsschichten. Dabei stellen sich für das Völkerrecht, insbesondere die menschenrechtlichen Regeln, schwierige Abgrenzungsprobleme: ab wann liegt im „Monitoring" des Kommunikationsverhaltens Einzelner ein Eingriff in ihre Menschenrechte? Binden diese Nachrichtendienste auch beim Handeln im Ausland? Zu berücksichtigen sein wird auch, dass die Gewinnung von nachrichtendienstlichen Erkenntnissen auch weiterhin ein legitimes Ziel staatlichen Handelns darstellt. Gerade die jüngsten politischen Entwicklungen im Osten Europas verdeutlichen, dass die Zeit zwischenstaatlicher Konflikte auch in Europa noch nicht passé ist und sich insofern auch das zwischenstaatliche Paradigma für staatliche Spionagetätigkeiten nicht gänzlich überlebt hat.

B. Völkerrechtliche Regeln zur Erhebung, Speicherung, Verarbeitung und Weitergabe von Daten

5. Hinsichtlich der einschlägigen völkerrechtlichen Normen ist zunächst zwischen zwei Sachbereichen zu differenzieren. Zum einen gibt es spezielle Regelungen über den Schutz von Daten, vor allem auf Ebene des Europarates. Zum anderen wird die nachrichtendienstliche Gewinnung und Verarbeitung von Daten auch von menschenrechtlichen Regeln erfasst.

I. Internationale Regeln zum Datenschutz

6. Im Hinblick auf spezifische Datenschutzregeln gibt es bislang keinen universellen Konsens über die rechtlichen Standards. Vielmehr gibt es auf dieser Ebene bisher nur unverbindliche Standards, etwa in Form der von der UN-Generalversammlung 1990 angenommenen Leitlinien für die Verarbeitung von computerbasierten persönlichen Daten.[5] Dies kommt zunächst dadurch zum Ausdruck, dass es kein multilaterales Vertragswerk zu diesem Komplex gibt. Angesichts verschiedener nationaler Verständnisse von Datenschutz kann auch nicht von einem völkergewohnheitsrechtlich akzeptierten Konzept des Datenschutzes ausgegangen werden.[6] Die Völkerrechtskommission der Vereinten Nationen (ILC) hat 2006 beschlossen, das Thema grenzüberschreitender Datenbewegungen in ihr „Long Term Working Programme" aufzunehmen.[7] Dem Vorschlag liegt die Annahme zugrunde, dass es einen „emerging trend" hin zu einem völkerrechtlichen Konzept des Datenschutzes gebe. Zu einem Konsens auf internationaler Ebene hinsichtlich der hier einschlägigen Standards sei es jedoch bisher nicht gekommen.[8] Angesichts dessen kann schon gar nicht von einem solchen Konsens im Hinblick auf die hier spezifisch interessierenden Fragen der nachrichtendienstlichen Erhebung und Verarbeitung von Daten gesprochen werden.

---

[5] Guidelines for the Regulation of Computerized Personal Data Files, UN Doc. A/RES/45/95 vom 14.12.1990, vgl. dazu Stephanie Schiedermaier, *Der Schutz des Privaten als internationales Grundrecht*, Tübingen 2012, S. 118 ff.; Kuner (Fn. 2), S. 26, 158.

[6] Vgl. Peter Malanczuk, Data, Transboundary Flow, International Protection, in: Rüdiger Wolfrum (Hrsg.), *Max Planck Encyclopedia of Public International Law*, Bd. II, 3. Aufl., Oxford 2012, S. 1033-1043, Rn. 26.

[7] International Law Commission, Report of the 58th Session, UN Doc. A/61/10, Annex D.

[8] In dem Projektvorschlag für die ILC heißt es dazu: „... it is ... an area, in which State practice is not yet extensive or fully developed." Die Kommission solle, "emerging trends in legal opinion and practice" identifizieren, vgl. ILC (Fn. 7), Rn. 12.

7. Im Rahmen des Europarates ist auf das 1981 angenommene Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten hinzuweisen (im Folgenden: „Europarat-Abkommen").[9] Das Abkommen steht auch Nicht-Mitgliedstaaten des Europarates offen. Von den sog. „five eyes"-Staaten ist das Vereinigte Königreich Vertragspartei. Die Bundesrepublik ist ebenfalls an das Abkommen gebunden.

8. Der Anwendungsbereich dieses Abkommens ist weit und allgemein bestimmt. Nach Art. 3 Abs. 1 des Europarat-Abkommens verpflichten sich die Vertragsparteien das „Übereinkommen auf automatisierte Dateien/Datensammlungen und automatische Verarbeitungen von personenbezogenen Daten im öffentlichen und privaten Bereich anzuwenden." Eine Bereichsausnahme für die nachrichtendienstliche Tätigkeit enthält das Abkommen nicht, womit seine Schutzstandards grundsätzlich auch auf geheimdienstliche Tätigkeiten Anwendung finden können, wenn es auch schwerlich vorstellbar ist, dass dies den Staaten beim Vertragsschluss als Anwendungsbereich des Abkommens vorschwebte. Genauso wenig ist es aber möglich, ex post den Vertragsparteien den Willen zuzuschreiben, wonach dieses Abkommen auf die Tätigkeiten von Nachrichtendiensten keine Anwendung finden würde.

9. Bei der Unterzeichnung oder bei einem späteren Beitritt in Form der Annahme oder Ratifikation können Staaten „bestimmte Arten von automatisierten Dateien/Datensammlungen mit personenbezogenen Daten" vom Anwendungsbereich des Vertrages ausnehmen, so es im innerstaatlichen Recht keine auf sie bezogenen Datenschutzbestimmungen gibt (vgl. Art. 3 Abs. 2 a) und b) des Europarat-Abkommens). Weder das Vereinigte Königreich noch die Bundesrepublik haben Tätigkeiten im geheimdienstlichen Bereich mit einer solchen Erklärung vom Anwendungsbereich ausgenommen.

10. In den Artikeln 5-8 des Europarat-Abkommens werden die materiellen Schutzstandards definiert, die insbesondere Grundsätze für die Datenerhebung und weitere Verwendung erhalten. Für den hier interessierenden Themenkomplex ist insbesondere relevant, dass die Daten

    - in rechtmäßiger Form erhoben werden müssen (Art. 5 a)),
    - sie für festgelegte und rechtmäßige Zwecke gespeichert sein und nicht so verwendet werden dürfen, dass es mit diesen Zwecken unvereinbar ist (Art. 5 bb)),
    - für die Zwecke, für die sie gespeichert sind, erheblich sein und nicht darüber hinausgehen dürfen (Art. 5 c)), sowie, dass
    - sie so aufbewahrt werden müssen, dass der Betroffene nicht länger identifiziert werden kann, als es die Zwecke, für die sie gespeichert sind, erfordern (Art. 5 e)).

    Art. 8 des Europarat-Abkommens sieht zudem Informationsrechte und Rechtsschutzmöglichkeiten des Einzelnen vor. Insgesamt ist zu berücksichtigen, dass sich die Konvention in erster Linie an die Vertragsparteien wendet und ihnen Pflichten zur Umsetzung der Konvention in innerstaatliches Recht auferlegt.

[9] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.1.1981, BGBl. 1985 II, S. 539.

11. Die in den Artikeln 5-8 des Europarat-Abkommens niedergelegten Rechte sind jedoch nicht schrankenlos gewährt. Vielmehr ist es nach Art. 9 Abs. 2 a) des Abkommens möglich, die Rechte aus Art. 5, 6 und 8 „zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten" einzuschränken. Damit es sich um eine zulässige Abweichung von den Standards des Abkommens handelt, ist nach Art. 9 Abs. 2 zu fordern, dass „sie durch das Recht der Vertragspartei vorgesehen und in einer demokratischen Gesellschaft" notwendig ist. Diese an die Terminologie der Europäischen Menschenrechtskonvention angelehnte Formulierung – siehe dazu unten bei Nr. 188 ff. – verdeutlicht, dass über die Zulässigkeit von Eingriffen in die Rechte des Abkommens letztlich eine Verhältnismäßigkeitsprüfung entscheiden muss.

12. Das Abkommen findet bei Tätigkeiten im Hoheitsgebiet der Vertragsparteien Anwendung, Art. 1 des Europarat-Abkommens. Sein Wortlaut schließt demnach eine extraterritoriale Anwendung – anders als menschenrechtliche Verträge – kategorisch aus.[10]

13. Ein 2001 angenommenes Zusatzprotokoll zu dem Abkommen[11] sieht in Art. 1 die Einrichtung von Kontrollstellen zur Durchsetzung des Abkommens vor. Art. 2 Abs. 1 des Zusatzprotokolls bestimmt weiter, „dass personenbezogene Daten an einen Empfänger, der der Hoheitsgewalt eines Staates oder einer Organisation untersteht, der beziehungsweise die nicht Vertragspartei des Übereinkommens ist, nur dann weitergegeben werden dürfen, wenn dieser Staat oder diese Organisation ein angemessenes Schutzniveau für die beabsichtigte Datenweitergabe gewährleistet". Allerdings kann von dieser Einschränkung nach Art. 2 Abs. 2 a), zweiter Spiegelstrich schon „wegen berechtigter öffentlicher Interessen" abgewichen werden, womit das Zusatzprotokoll dem Austausch von Daten durch Nachrichtendienste kaum Grenzen setzen dürfte.

II. Menschenrechtliche Regeln

14. Im menschenrechtlichen Bereich ist die Erhebung und Verarbeitung von Daten Gegenstand des in verschiedenen völkerrechtlichen Verträgen wie dem Internationalen Pakt über bürgerliche und politische Rechte (IPbpR)[12] und der Europäischen Menschenrechtskonvention (EMRK)[13] gewährleisteten Rechts auf Privatsphäre (Art. 17 IPbpR, Art. 8 EMRK). Dieses wird auch von Art. 12 der Allgemeinen Erklärung der Menschenrechte (AEMR)[14] geschützt, die als Resolution der UN-Generalversammlung zwar keine Rechtsverbindlichkeit genießt, jedoch in weiten Teilen als Ausdruck des Völkergewohnheitsrechts angesehen wird.[15] Im Folgenden soll zunächst dem materiellen

---

[10] Kuner (Fn. 2), S. 129. Reformbemühungen seitens des Europarats und anderer „Stakeholder" wollen dies jedoch ändern und an menschenrechtliche Konzepte der Ausübung von Hoheitsgewalt anknüpfen, vgl. ebd., S. 138-141.

[11] Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr vom 8.11.2001, BGBl. 2002 II, S. 1882, 1887.

[12] Internationaler Pakt über bürgerliche und politische Rechte vom 19.12.1966, BGBl. 1973 II, S. 1534.

[13] Konvention zum Schutz der Menschenrechte und Grundfreiheiten vom 4.11.1950, in der zuletzt geänderten Fassung BGBl. 2010 II, S. 1198.

[14] Allgemeine Erklärung der Menschenrechte vom 10.12.1948, UN Doc. A/RES/217 A (III).

[15] Christian Tomuschat, *Human Rights – Between Idealism and Realism*, 2. Aufl., Oxford 2008, S. 37 f.

Schutzstandard dieser Regeln nachgegangen werden, bevor die Frage der extraterritorialen Anwendbarkeit thematisiert wird.

15. Allgemein kann zum Verhältnis zwischen einem Recht auf Datenschutz und dem Recht auf Privatsphäre gesagt werden, dass diese sich zwar überschneiden, aber nicht deckungsgleich sind.[16] Die Integrität persönlicher Daten ist ein wichtiger Aspekt des Schutzes auf Privatsphäre, die aber einen darüber hinaus zielenden weiteren Anwendungsbereich hat, der in der Spruchpraxis internationaler Gerichte und Ausschüsse in einer Vielzahl von Fallgruppen ausdifferenziert wurde.[17]

16. Dass das Recht auf Privatsphäre auch im Internet – „online wie offline" – gilt, ist von den Mitgliedstaaten der UN durch die im Konsens angenommene Generalversammlungsresolution „The right to privacy in the digital age" im Dezember 2013 bekräftigt worden.[18] Ohne Einordnung konkreter Vorgänge kann dieser Resolution entnommen werden, dass es einen Konsens in der Frage gibt, dass staatliche Überwachungsmaßnahmen zu Verletzungen des Rechts auf Privatsphäre nach Art. 12 AEMR und Art. 17 IPbpR führen können. Der UN-Menschenrechtsausschuss (MRA) hat zudem 2014 im Rahmen des Staatenberichtsverfahrens seine Sorge über Verletzungen des Paktes durch Überwachungsmaßnahmen der NSA im In- und Ausland zum Ausdruck gebracht.[19] So hat der Ausschuss den Vereinigten Staaten empfohlen, dass sie alle notwendigen Maßnahmen treffen sollen, dass Überwachungsmaßnahmen sowohl in den Vereinigten Staaten als auch im Ausland im Einklang mit Art. 17 IPbpR stehen.[20] Schon im Frühjahr 2013 hatte der Sonderberichterstatter der UN für den Schutz der Meinungsfreiheit, Frank La Rue auf die neuen Herausforderungen für den Schutz der Privatsphäre durch die gesteigerten Möglichkeiten der staatlichen Überwachung moderner Kommunikationsmittel hingewiesen.[21]

17. Zur Schutzrichtung der menschenrechtlichen Normen ist festzuhalten, dass sich staatliche Stellen nicht auf die Abwehrdimension der Menschenrechte berufen können, da sie insoweit keine Träger von Grund- und Menschenrechten sind. Dies bedeutet allerdings nicht, dass sich etwa eine Regierungschefin gegenüber Abhörmaßnahmen eines anderen Staates gar nicht auf ihre Privatsphäre berufen kann.[22] Auch Regierungsmitglieder genießen als Privatpersonen den Schutz der Menschenrechte. Allerdings können sich die Standards für die Rechtfertigung von Eingriffen in diese Rechte verändern, wenn die Inhalte von staatlicher und privater Kommunikation nicht klar getrennt werden können.

---

[16] Schiedermaier (Fn. 5), S. 239 f.; Kuner (Fn. 2), S. 19.

[17] Vgl. nur für Art. 8 EMRK Juliane Pätzold, in: Ulrich Karpenstein/Franz C. Mayer (Hrsg.), *EMRK-Kommentar*, München 2012, Art. 8, Rn. 5 ff.; zu Art. 17 IPbpR Sarah Joseph/Melissa Castan, *The International Covenant on Civil and Political Rights – Cases, Materials and Commentary*, 3. Aufl., Oxford 2013, S. 533 ff.

[18] UN Doc. A/RES/68/167 vom 18.12.2013.

[19] Human Rights Committee, Concluding Observations on the Fourth Report of the United States of America, adopted by the Committee at its 110th session, 10-28 March 2014, advance unedited version, Rn. 22.

[20] Ebd.

[21] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. A/HRC/23/40 vom 17.4.2013.

[22] Vgl. auch Stefan Talmon, Tapping the German Chancellor's Cell Phone and Public International Law, *Cambridge Journal of International and Comparative Law Blog*, 6.11.2013, abrufbar unter http://cjicl.org.uk/2013/11/06/tapping-german-chancellors-cell-phone-public-international-law/ (zuletzt aufgerufen am 26.5.2014).

III. Konkretisierung der Schutzstandards durch den EGMR

18. Der Europäische Gerichtshof für Menschenrechte hat die sich aus Art. 8 EMRK für nachrichtendienstliche Überwachungsmaßnahmen ergebenden Standards in verschiedenen Entscheidungen näher konkretisiert.[23] Danach werden Telefongespräche und andere Formen der Telekommunikation von den Begriffen „Privatleben" und „Korrespondenz" i.S.v. Art. 8 EMRK erfasst.[24] Der Schutzumfang von Art. 8 EMRK bezieht sich dabei auch auf den Datenschutz. Der Gerichtshof hat in seiner Rechtsprechung hervorgehoben, dass die Verwahrung von Informationen über das Privatleben einer Person in einem öffentlichen Register in den Anwendungsbereich von Art. 8 Abs. 1 EMRK fällt. In diesem Zusammenhang greift der Gerichtshof zur Auslegung von Art. 8 Abs. 1 EMRK auch auf das Europarat-Abkommen zum Datenschutz von 1981 zurück, womit die dort niedergelegten datenschutzrechtlichen Standards mittelbar auch für die Konkretisierung der EMRK Bedeutung gewinnen.[25]

19. Schon die bloße Existenz von Gesetzen, die eine geheime Überwachung des Fernmeldeverkehrs gestatten, stellt für alle potentiell von der Überwachung betroffenen Personen eine Bedrohung dar und betrifft ihre Kommunikationsfreiheit. Ein Eingriff in Art. 8 EMRK liegt schon durch die bloße Existenz eines solchen Überwachungssystems vor.[26]

20. Auch in der weiteren Verarbeitung und Übermittlung von Daten kann ein Eingriff in Art. 8 EMRK liegen, da solche Maßnahmen die Grundlage für weiteres staatliches Handeln gegenüber den Betroffenen darstellen können.[27]

21. Nach Art. 8 Abs. 2 EMRK bedürfen Eingriffe einer gesetzlichen Regelung. Solche Regeln müssen nach der Rechtsprechung des EGMR für die betroffenen Personen zugänglich sein.[28] Es muss vorhersehbar sein, welche Folgen das Gesetz für die betroffenen Personen hat. Da Überwachungsmaßnahmen ihrer Natur nach geheimhaltungsbedürftig sind, hat der Gerichtshof in seiner Rechtsprechung Mindeststandards bezeichnet, die eingehalten werden müssen, um eine willkürliche Ausdehnung von Überwachungsmaßnahmen zu verhindern.[29] Die gesetzlichen Regelungen müssen insbesondere eine Aufzählung der Straftaten enthalten, zu deren Zweck strategische Überwachungsmaßnahmen angeordnet werden dürfen. Gleichwohl ist es nicht erforderlich, dass jeder einzelne Straftatbestand explizit Erwähnung findet. In einem Verfahren gegen das Vereinigte Königreich hat der Gerichtshof es auch für ausreichend erachtet, wenn eine gesetzliche Grundlage bestimmt, dass der Secretary of

---

[23] EGMR, *Weber und Saravia/Deutschland*, Beschwerde-Nr. 54934/00, Entscheidung über die Zulässigkeit vom 29.6.2006 = NJW 2007, 1433. Vgl. außerdem EGMR, *Klass u.a./Deutschland*, Beschwerde-Nr. 5029/71, Urteil vom 6.9.1978 = NJW 1979, 1755; EGMR, *Rotaru/Rumänien*, Beschwerde-Nr. 28341/95, Urteil vom 4.5.2000 (GK); EGMR, *Liberty u.a./Vereinigtes Königreich*, Beschwerde-Nr. 58243/00, Urteil vom 1.7.2008; EGMR, *Kennedy/Vereinigtes Königreich*, Beschwerde-Nr. 26839/05, Urteil vom 18.5.2010; zusammenfassend aus der Literatur Schiedermaier (Fn. 5), S. 225 ff.

[24] EGMR, *Klass u.a./Deutschland* (Fn. 23), Rn. 41; EGMR, *Weber und Saravia/Deutschland* (Fn. 23), Rn. 77.

[25] EGMR, *Rotaru/Rumänien* (Fn. 23), Rn. 43.

[26] EGMR, *Klass u.a./Deutschland* (Fn. 23), Rn. 41; EGMR, *Weber und Saravia/Deutschland* (Fn. 23), Rn. 78.

[27] EGMR, *Weber und Saravia/Deutschland* (Fn. 23), Rn. 79.

[28] EGMR, *Weber und Saravia/Deutschland* (Fn. 23), Rn. 84, 92 f.

[29] EGMR, *Klass u.a./Deutschland* (Fn. 23), Rn. 50; EGMR, *Malone/Vereinigtes Königreich*, Beschwerde-Nr. 8691/79, Urteil vom 2.8.1984, Rn. 67; EGMR, *Leander/Schweden*, Beschwerde-Nr. 9248/81, Urteil vom 26.3.1987, Rn. 51; EGMR, *Weber und Saravia/Deutschland* (Fn. 23), Rn. 93.

State Überwachungsmaßnahmen anordnen kann, wenn es im Interesse der nationalen Sicherheit oder zur Verhinderung schwerer Straftaten notwendig sei.[30] Ferner ist nach dem EGMR die Beschreibung der Personengruppen gesetzlich zu bestimmen, deren Kommunikation überwacht werden darf. Schließlich muss die Begrenzung der Dauer der Abhörmaßnahme und das Verfahren der Auswertung, Verwendung und Speicherung der Daten nebst den Umständen, unter denen die erlangten Daten wieder gelöscht werden müssen, gesetzlich geregelt sein.[31]

22. Weiterhin müssen Eingriffe einem legitimen Ziel i.S.v. Art. 8 Abs. 2 EMRK dienen und „in einer demokratischen Gesellschaft notwendig" sein. Der Gerichtshof erkennt dabei grundsätzlich an, dass auch in einer „demokratischen Gesellschaft" die Existenz von Geheimdiensten berechtigt sein kann. Ermächtigungen zu einer geheimen Überwachung seien aber nur insoweit zu tolerieren, wie es unbedingt notwendig sei, u die demokratischen Institutionen des Staates zu schützen.[32] Dabei lässt der EGMR grundsätzlich auch Maßnahmen der „strategischen Überwachung", d.h. nicht auf konkrete Einzelpersonen bezogene Überwachungsmaßnahmen, zu, wenn und soweit „angemessene und wirksame Garantien gegen Missbrauch" vorgesehen sind.[33]

IV. Konkretisierung der Schutzstandards durch den MRA

23. Ähnliche Standards gelten auch für die Auslegung des Art. 17 IPbpR.[34] Nach der vom MRA schon im Jahre 1988 in seinem „General Comment" Nr. 16 vorgenommen Auslegung des Art. 17 IPbpR schützt diese Bestimmung auch vor elektronischen Überwachungsmaßnahmen, der Aufzeichnung von Telefonaten und anderer Form von Kommunikation. Jedenfalls muss nach dem MRA ein gesetzlicher Rahmen geschaffen werden, der diese Maßnahmen reguliert.[35]

24. Die Spruchpraxis des MRA ist in diesem Bereich im Übrigen noch nicht vergleichbar entwickelt wie diejenige des EGMR. In seiner Stellungnahme zum Staatenbericht der Vereinigten Staaten hat der MRA jedoch sehr ähnliche Kriterien zugrunde gelegt. Insbesondere hat er empfohlen, dass Maßnahmen getroffen werden sollten, um sicherzustellen, dass jeder Eingriff in das Recht auf Privatsphäre im Einklang mit rechtstaatlichen Grundsätzen (principle of legality) stattfinden und verhältnismäßig sein müsse, unabhängig von der Staatsangehörigkeit der Betroffenen oder ihrem Aufenthaltsort. Zudem müssten Eingriffe durch ein Gesetz vorgesehen sein, dass

    - öffentlich zugänglich sein müsse,

---

[30] EGMR, *Kennedy/Vereinigtes Königreich* (Fn. 23), Rn. 159.

[31] EGMR, *Weber und Saravia/Deutschland* (Fn. 23), Rn. 95.

[32] EGMR, Klass u.a./Deutschland (Fn. 23), Rn. 42; EGMR, *Rotaru/Rumänien* (Fn. 23), Rn. 47.

[33] EGMR, *Weber und Saravia/Deutschland* (Fn. 23), Rn. 106.

[34] Zu den Parallelen hinsichtlich der Auslegung von EMRK und IPbpR siehe Schiedermaier (Fn. 5), S. 308 ff.; kritisch hinsichtlich der Existenz eines internationalen Rechts auf Schutz der Privatsphäre hingegen Eric A. Posner, Statement to the Privacy & Civil Liberties Oversight Board, 14 March 2014, S. 2, abrufbar unter http://www.pclob.gov/meetings-and-events/2014meetingsevents/19-march-2014-public-hearing (zuletzt aufgerufen am 26.5.2014).

[35] Human Rights Committee, General Comment 16 (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, UN Doc. HRI/GEN/1/Rev 1, 21 (1994).

- Bestimmungen enthalte, welche die Voraussetzungen bestimmten, unter denen Überwachungsmaßnahmen zulässig seien, die zudem hinreichend bestimmt hinsichtlich der ermächtigenden Tatbestände seien,
- Kategorien für Personengruppen aufstelle, die von Überwachungsmaßnahmen betroffen sein könnten,
- zeitliche Grenzen für die Überwachung aufstelle,
- Bestimmungen für die Speicherung und Benutzung von Daten enthalte und
- wirksame Garantien gegen einen Missbrauch der Ermächtigungsnormen vorsehe.

Das gegenwärtige System der Geheimdienstkontrolle in den Vereinigten Staaten solle zudem reformiert werden, genauso wie sichergestellt werden solle, dass betroffene Personen einen Zugang zu wirksamen Beschwerdemechanismen hätten.[36] All diese Punkte sind vom Komitee im Modus von Empfehlungen formuliert worden, womit nicht zwangsläufig davon ausgegangen werden kann, dass alle Mitglieder des Ausschusses der Auffassung sind, dass es sich um rechtlich bindende Verpflichtungen der Vereinigten Staaten entspricht. Gleichwohl kann der Stellungnahme die Position des MRA entnommen werden, dass eine solche Reform des US-amerikanischen Geheimdienstwesens und der entsprechenden Programme der NSA am ehesten den Verpflichtungen aus dem Pakt entsprechen würde.

V. Die Schutzpflichtendimension

25. Sowohl Art. 17 IPbpR als auch Art. 8 EMRK kann zudem eine Schutzpflichtendimension gegenüber privaten Akteuren und fremden Staaten entnommen werden. Der MRA hat in seinem General Comment Nr. 16 festgehalten, dass die Vertragsparteien des Paktes nicht nur unter einer Verpflichtung stünden, nicht selber in die Privatsphäre von Individuen einzugreifen, sondern auch einen gesetzgeberischen Rahmen zu schaffen, der die Begehung von durch Art. 17 IPbpR verbotenen Maßnahmen verhindere.[37]
26. Hinsichtlich der Reichweite der Schutzpflichtendimension ist zu beachten, dass – ähnlich wie im nationalen Verfassungsrecht – den staatlichen Stellen in aller Regel eine erhebliche Einschätzungsprärogative eingeräumt wird, wie sie ihrem Schutzauftrag nachkommen werden.[38]
27. Der Rechtsprechung des EGMR lässt sich allerdings entnehmen, dass in bestimmten Fällen eine Verletzung der Schutzpflicht vorliegen kann, wenn eine Vertragspartei der EMRK einen anderen Staat oder nicht-staatliche Akteuren in der Begehung einer Menschenrechtsverletzung unterstützt. Solche Unterstützungshandlungen stellen sich dann zwar nicht notwendigerweise als eigenständiger Eingriff in die EMRK-Rechte dar. Zugleich können sie aber als Ausdruck dafür zu werten sein, dass ein Staat seine Schutzpflichten nicht erfüllt hat. Insofern können auch Formen der nachrichtendienstlichen Kooperation zu einer

[36] Human Rights Committee, Concluding Observations (Fn. 19), Rn. 22, Empfehlungen a)-e).

[37] Human Rights Committee, General Comment 16 (Fn. 35), Rn. 9.

[38] Vgl. Thilo Marauhn/Judith Thorn, Privat- und Familienleben, in: Oliver Dörr/Rainer Grote/Thilo Marauhn (Hrsg.), *Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz*, Bd. I, 2. Aufl., Tübingen 2013, S. 868-956, Rn. 25.

Verurteilung durch den EGMR unter Schutzpflichtgesichtspunkten führen.[39] Diese Rechtsprechung greift einen allgemeinen Gedanken des völkerrechtlichen Haftungsrechts (der Staatenverantwortlichkeit) auf, wonach Staaten auch für die Unterstützung rechtswidriger Akte anderer Staaten zur Rechenschaft gezogen werden können.[40] Es wird im Einzelfall dann darauf ankommen, welches Ausmaß die nachrichtendienstliche Kooperation hatte und mit welchem Zweck die Daten an die Dienste anderer Staaten weitergegeben wurden.

VI. Extraterritoriale Anwendbarkeit der menschenrechtlichen Garantien?

28. Sowohl für den Schutz nach IPbpR und EMRK ist – neben der Ermittlung der materiellen Schutzstandards – jeweils im Einzelfall zu bestimmen, ob die Normen zum Schutz der Privatsphäre überhaupt Anwendung auf die nachrichtendienstliche Erfassung und weitere Verarbeitung von Telekommunikationsdaten und Internetnutzung finden.[41] Nach Art. 1 EMRK sichern die Hohen Vertragsparteien die Rechte der Konvention allen ihrer Hoheitsgewalt unterstehenden Personen zu. Art. 2 Abs. 1 IPbpR bestimmt, dass jeder Vertragsstaat sich verpflichtet, die in diesem Pakt anerkannten Rechte zu achten und sie allen in seinem Gebiet befindlichen und seiner Hoheitsgewalt unterstehenden Personen zu gewährleisten.

29. Unproblematisch den beiden Verträgen unterfallen Aktivitäten mit denen Staaten auf ihrem eigenen Staatsgebiet Zugriff auf Internet- und Telekommunikationsdaten gewinnen. Wenn also ein Staat auf Daten zugreift, die auf Servern gespeichert sind, die sich in seinem Territorium befinden, ist in dem Zugriff eine Ausübung von Hoheitsgewalt zu erkennen (wie beim PRISM-Programm der NSA).[42] Dies gilt auch unabhängig von der Staatsangehörigkeit der betroffenen Personen.[43]

---

[39] Vgl. dazu die Entscheidung EGMR, *el-Masri/Ehemalige jugoslawische Republik Mazedonien*, Beschwerde-Nr. 39630/09, Urteil vom 13.12.2012 (GK), = NVwZ 2013, 631 (in Teilen abgedruckt), in der es um das Zusammenwirken von mazedonischen und US-amerikanischen Sicherheitsbehörden ging. Auch wenn die Konstellation der sog. „extraordinary renditions" sicher einen Sonderfall betrifft, signalisiert das Urteil eine Bereitschaft des Gerichtshofs, sehr weitreichende Konsequenzen aus der Unterstützung von Menschenrechtsverletzungen durch Drittstaaten zu ziehen.

[40] Vgl. Art. 16 der 2001 von der Völkerrechtskommission der Vereinten Nationen angenommenen Artikel zur Staatenverantwortlichkeit, abgedruckt im Anhang von UN Doc. A/RES/56/83 vom 12.12.2001; zur Beihilfe näher Helmut Philipp Aust, *Complicity and the Law of State Responsibility*, Cambridge 2011, insb. zum Zusammenhang mit menschenrechtlichen Schutzpflichten ebd., S. 390 ff.

[41] Vgl. dazu Wolfgang Ewer/Tobias Thienel, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, *NJW* 2014, 30 (32 f.); Marko Milanovic, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, *Harvard International Law Journal*, i.E., abrufbar unter http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485 (zuletzt aufgerufen am 25.5.2014); Talmon (Fn. 22); zu allgemein in dieser Frage Stefanie Schmahl, Effektiver Rechtsschutz gegen Überwachungsmaßnahmen ausländischer Geheimdienste?, *JZ* 2014, 220 (227).

[42] So auch Wewer/Thienel (Fn. 41), S. 31.

[43] Die US-amerikanische Rechtsauffassung trägt dem allerdings nur teilweise Rechnung, insoweit als sie den Schutz durch das Vierte Amendment der Verfassung und der Verfahrensbestimmungen des Foreign Intelligence Surveillance Act zwar nicht nur amerikanischen Staatsangehörigen zubilligt, sondern auch der breiteren Kategorie von "US persons", d.h. Personen, die einen Aufenthaltstitel für die USA besitzen oder sich physisch auf dem US-amerikanischen Staatsgebiet aufhalten. „Non US-persons" sollen dagegen nicht dem verfassungsrechtlichen Schutz unterfallen; vgl. Peter Margulies, The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism, *Fordham Law Review* 82 (2014), S. 2137-2167 (2137); Klaus-

30. Auch das Anzapfen von transatlantischen Telekommunikationskabeln auf dem eigenen Staatsgebiet (wie es für das Tempora-Programm des britischen Geheimdienstes GCHQ berichtet wird) stellt eine Ausübung von Hoheitsgewalt auf dem eigenen Staatsgebiet dar. In einer gegen das Vereinigte Königreich gerichteten und erfolgreichen Individualbeschwerde, in der es um Maßnahmen der strategischen Auslandsüberwachung ging, von denen – mutmaßlich – auch Nichtregierungsorganisationen mit Sitz im irischen Dublin betroffen waren, hat der EGMR die Frage, ob hier Hoheitsgewalt ausgeübt wurde, dementsprechend nicht weiter problematisiert.[44] In solchen Fällen geht es letztlich nicht um eine extraterritoriale Anwendbarkeit der Konvention, sondern vielmehr um territorial basiertes Handeln, welches Effekte jenseits der eigenen Staatsgrenzen hervorruft.[45] Dass in solchen Fällen das Handeln eine Ausübung von Hoheitsgewalt darstellen kann, hat der Gerichtshof auch in anderen Konstellationen anerkannt.[46] Zudem gilt grundsätzlich eine Vermutung dafür, dass die Staaten in ihrem eigenen Staatsgebiet Hoheitsgewalt ausüben.[47] Gegenüber Überwachungsmaßnahmen, die ihren Ausgang vom jeweils eigenen Staatsgebiet haben, müsste also dargelegt werden, warum es sich ausnahmsweise nicht um eine Ausübung von Hoheitsgewalt handelt.

31. Schwieriger stellt sich die Situation demgegenüber dar, wenn staatliche Organe auf fremdem Staatsgebiet Daten erheben und weiterverarbeiten.[48] Anknüpfend an die Formulierung des Art. 2 Abs. 1 IPbpR wird es vor allem von Israel und den Vereinigten Staaten in Abrede gestellt, dass die Rechte des IPbpR auch bei staatlichem Handeln jenseits des eigenen Staatsgebietes Anwendung finden.[49] Diese beiden Staaten verstehen die Bestimmung des Art. 2 Abs. 1 IPbpR so, dass „in ihrem Staatsgebiet" und „unter ihrer Hoheitsgewalt"

Ferdinand Gärditz/Carl-Friedrich Stuckenberg, Vorratsdatenspeicherung à l'Américaine – Zur Verfassungsmäßigkeit der Sammlung von Telefonverbindungsdaten in den USA, *JZ* 2014, S. 209-219 (211).

[44] EGMR, *Liberty u.a./Vereinigtes Königreich* (Fn. 23).

[45] Dabei handelt es sich *nicht* um einen Anwendungsfall der umstrittenen „effects doctrine", mit welcher Staaten ihre legislativen Zuständigkeiten (*jurisdiction to prescribe*) auszudehnen suchen, indem sie Auslandssachverhalte ihrem eigenen Recht unterstellen, weil sie Auswirkungen in ihrem eigenen Bereich zeitigt. Hier ist die Konstellation entgegengesetzt: es geht um eine fortwirkende Bindung an die menschenrechtlichen Verpflichtungen bei Handlungen im eigenen Staatsgebiet, welche Wirkungen im Ausland nach sich ziehen. Zur „effects doctrine" siehe James Crawford, *Brownlie's Principles of Public International Law*, 8. Aufl., Oxford 2012, S. 462-464.

[46] EGMR, *Drozd und Janousek/Frankreich und Spanien*, Beschwerde-Nr. 12747/87, Urteil vom 26.6.1992, Rn. 91: „The term "jurisdiction" is not limited to the national territory of the High Contracting Parties; their responsibility can be involved because of acts of their authorities producing effects outside their own territory." Eine prominente Kategorie der außerhalb des eigenen Staatsgebiets eintretenden Wirkungen von Handlungen auf dem eigenen Territorium sind Auslieferungsfälle, in denen es um den von Art. 3 EMRK geschützten Grundsatz des *non-refoulement* geht, vgl. EGMR, *Soering/Vereinigtes Königreich*, Beschwerde-Nr. 14038/88, Urteil vom 7.7.1989 = NJW 1990, 2183; EGMR, *Saadi/Italien*, Beschwerde-Nr. 37201/06, Urteil vom 28.2.2008 (GK) = NVwZ 2008, 1330.

[47] EGMR, *Ilascu u.a./Moldawien und Russland*, Beschwerde-Nr. 48787/99, Urteil vom 8.7.2004 (GK) = NJW 2005, 1849, Rn. 312.

[48] Ablehnend hinsichtlich der Frage, ob in solchen Fällen Hoheitsgewalt ausgeübt wird John B. Bellinger III, Testimony before the Private & Civil Liberties Oversight Board, 19 March 2014, abrufbar unter http://www.pclob.gov/meetings-and-events/2014meetingsevents/19-march-2014-public-hearing (zuletzt aufgerufen am 26.5.2014); Posner (Fn. 34).

[49] Vgl. zu Israel: Human Rights Committee, Concluding Observations of the Human Rights Committee on Israel, UN Doc. CCPR/C/ISR/CO/3 vom 3.9.2010, Rn. 5; zu den Vereinigten Staaten: Human Rights Committee, Concluding Observations (Fn. 19), Rn. 4.

kumulative und damit aufeinander bezogene Voraussetzungen sind. In einer Stellungnahme vor dem „Private & Civil Liberties Oversight Board" hat ein führender US-amerikanischer Rechtswissenschaftler dies so umschrieben:

> „The longstanding U.S. view is that the ICCPR protects people from abuses by their own governments, not from actions by foreign governments with respect to individuals outside the territory over which the government has jurisdiction."[50]

Sowohl der IGH als auch der MRA haben jedoch bekräftigt, dass die Verpflichtungen des Paktes auch jenseits des eigenen Staatsgebiets Anwendung finden und sich für eine alternative Lesart der Bestimmung des Art. 2 Abs. 1 IPbpR ausgesprochen.[51] Danach kann der IPbpR zur Anwendung kommen, wenn es entweder um Handeln auf dem eigenen Staatsgebiet geht oder wenn sich Individuen unter der Hoheitsgewalt eines Staates befinden. Für die EMRK hat sich eine im Einzelnen nicht immer konsistente und stark von Einzelfällen geprägte Rechtsprechung des EGMR herausgebildet.[52] Auch in der Literatur wird überwiegend davon ausgegangen, dass die menschenrechtlichen Verpflichtungen auch bei extraterritorialem Handeln zur Anwendung kommen.[53]

32. In dem schon erwähnten Fall Weber und Saravia gegen Deutschland vor dem EGMR hatte die Bundesregierung argumentiert, dass die Beschwerdeführer – da in Argentinien lebend – nicht deutscher Hoheitsgewalt unterfallen würden, wenn sie von Maßnahmen der Auslandsüberwachung des BND betroffen seien. Der EGMR ging dieser Frage in der Entscheidung aus prozessökonomischen Gründen aus dem Weg und wies die Beschwerde aus anderen Gründen als unzulässig ab, ohne über die Frage des Vorliegens von Hoheitsgewalt zu entscheiden.[54]

33. Auch wenn in dieser Frage im Einzelnen vieles ungeklärt ist, kann festgehalten werden, dass der zentrale Begriff für die Bestimmung der Frage, ob ein Staat jenseits seines eigenen Staatsgebiets Hoheitsgewalt ausübt, derjenige der „effektiven Kontrolle" ist – jedenfalls, wenn man sich nicht der Auffassung Israels und der Vereinigten Staaten anschließt. Die Kontrolle ist dabei entweder auf ein Gebiet als solches bezogen (*effective overall control*) oder auf Formen der Herrschaftsausübung gegenüber Individuen (*state agent authority and control*). Die dabei bisher in der Rechtsprechung vorhandenen Fallgruppen sind nur begrenzt weiterführend, da es sich vor allem um Konstellationen des Einsatzes bewaffneter Gewalt handelt.[55] Wenn es um den Eingriff in die Privatsphäre geht, kann die „effektive Kontrolle" eines Staates über den Einzelnen schon begriffsnotwendig nicht die gleiche Intensität

---

[50] Posner (Fn. 34), S. 2.

[51] Human Rights Committee, *Lopez Burgos v Uruguay*, communication No. R.12/52, Final views of 29 July 1981, Rn. 12.3; 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 (2004), Rn. 10; ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, ICJ Rep. 2004, 136, Rn. 111.

[52] Zusammenfassend EGMR, *Al Skeini u.a./Vereinigtes Königreich*, Beschwerde-Nr. 55721/07, Urteil vom 7.7.2011 (GK), Rn. 131 ff.

[53] Vgl. allgemein zu dieser Frage Tomuschat (Fn. 15), S. 126 ff.; eingehend Marko Milanovic, *Extraterritorial Application of Human Rights Treaties*, Oxford 2011; kritisch dazu Samantha Besson, The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to, *Leiden Journal of International Law* 25 (2012), 857-884.

[54] EGMR, *Weber und Saravia/Deutschland* (Fn. 23), Rn. 66, 72.

[55] Vgl. auch Kuner (Fn. 2), S. 129.

erlangen, wie dies bei einer Freiheitsberaubung, unmenschlichen Behandlung oder gar Folterung und Tötung der Fall ist.[56] Was „effektive Kontrolle" im Kontext von Art. 8 EMRK und Art. 17 IPbpR bedeutet, bedarf somit einer spezifischen, auf das Grundrecht des Schutzes der Privatsphäre bezogenen Überlegung.

34. Da die Rechtsprechung des EGMR zur Frage der extraterritorialen Anwendbarkeit der EMRK stark vom Einzelfall abhängig ist, kann davon ausgegangen werden, dass dies auch in Bezug auf die nachrichtendienstliche Gewinnung von Daten außerhalb des eigenen Staatsgebiets der Fall sein wird. Aus der bisherigen Rechtsprechung verallgemeinerbar ist die Erwägung, dass effektive Kontrolle ein mehrdimensionales Merkmal ist: einerseits knüpft es an die faktische Möglichkeit des betroffenen Staates an, die Menschenrechte auch wirklich gewährleisten zu können. Deshalb ist effektive Kontrolle regelmäßig dann gegeben, wenn ein Staat z.B. Besatzungsmacht in einem anderen Staat ist.[57] Ist diese generalisierte Kontrolle andererseits weniger stark, wird dieses Defizit durch eine stärkere Verbindung zwischen handelndem Staat und betroffenem Individuum kompensiert, so etwa wenn bewaffnete Agenten eines Staates eine Person im Territorium eines Drittstaates entführen.[58]

35. Beide Gesichtspunkte – generalisierte Kontrolle über eine Vielzahl von Sachverhalten, punktuelle Kontrolle über ein Individuum – können auch für die hier interessierenden Fragen fruchtbar gemacht werden. Je genereller die Kontrolle eines Staates über den Internetverkehr wird, desto eher wird man ihm entgegen halten können, dass diese Form der staatlichen Aktivität nicht ohne menschenrechtliche Bindungen einhergeht. Dabei sollte – eine Wertung aus dem Bereich des Datenschutzrechts aufnehmend – der reine Transit von Daten durch über ein Territorium laufende Leitungen nicht ausreichen, um die Ausübung von Hoheitsgewalt zu begründen.[59] Umgekehrt: je stärker ein bestimmtes Individuum in das Blickfeld eines Nachrichtendienstes gerät und je mehr es durch diese Maßnahmen zur Erstellung eines Persönlichkeitsbildes kommt, desto eher kann im Vorliegen einer „virtuellen Kontrolle"[60] über die Daten einer Person auch das Vorliegen von effektiver Kontrolle über diese erblickt werden. Diese Unterscheidung kann auch die verschiedenen Dimensionen von Eingriffen in das Recht auf den Schutz der Privatsphäre aufnehmen. Der EGMR hat in seiner Rechtsprechung festgehalten, dass nicht nur die Erfassung von Daten einen Eingriff darstellt, sondern auch jede weitere Verarbeitung, Verwendung und Weitergabe von Daten. Hier bietet sich die Möglichkeit für eine Differenzierung anhand von territorialen wie auch materiellen Gesichtspunkten an. Kann eine außerhalb des staatlichen Territoriums stattfindende Überwachungsmaßnahme, die nur allgemein den Internetverkehr kontrolliert, vielleicht nicht in jedem Einzelfall als Ausübung von Hoheitsgewalt angesehen werden, wandelt sich der Charakter der staatlichen Maßnahmen spätestens dann, wenn die Daten in

---

[56] In diese Richtung auch Margulies (Fn. 43), S. 2150.

[57] Für eine solche Konstellation EGMR, *Loizidou/Türkei*, Beschwerde-Nr. 15318/89, Urteil vom 23.3.1995, Rn. 62.

[58] Vgl. hierzu EGMR, *Öcalan/Türkei*, Beschwerde-Nr. 46221/99, Urteil vom 12.3.2003 und Urteil der Großen Kammer vom 12.5.2005.

[59] Vgl. zum reinen Transit von Daten Kuner (Fn. 2), S. 15; anders als hier (Transit von Daten reicht aus): Margulies (Fn. 43), S. 2151; Laura Pitter, Comments of Human Rights Watch, Privacy and Civil Liberties Board Hearing, 19 March 2014, S. 9, abrufbar unter http://www.pclob.gov/meetings-and-events/2014meetingsevents/19-march-2014-public-hearing (zuletzt aufgerufen am 26.5.2014).

[60] Dazu Anne Peters, Surveillance Without Borders? The Unlawfulness of the NSA Panopticon, Part II, *EJIL:Talk!* vom 4. November 2013, abrufbar unter http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/ (zuletzt aufgerufen am 2. Mai 2014); Margulies (Fn. 43), S. 2150.

Datenbanken auf dem jeweiligen Staatsgebiet des Staates gespeichert und weiterverarbeitet werden. Erfolgt die weitere Verarbeitung jenseits des eigenen Staatsgebiets ist zumindest dann vom Vorliegen von Hoheitsgewalt auszugehen, wenn auf spezifische Datensätze zugegriffen wird, die einem Individuum zugeordnet werden können.

36. Diese Unterscheidung ist auch im Lichte der vorliegenden Erkenntnisse geeignet, die Praxis der nachrichtendienstlichen Informationsbeschaffung sinnvoll zu erfassen. Die besonders kontroversen Spähprogramme „PRISM“ und „Tempora“ basieren jeweils auf Handlungen mit einem eindeutigen Bezug zum Staatsgebiet der Vereinigten Staaten bzw. des Vereinigten Königreichs. Wird – wie z.B. im Rahmen der strategischen Auslandsüberwachung des BND – Satellitenbasierte Kommunikation abgehört und ausgewertet, findet dies ebenfalls vielfach ausgehend von technischen Einrichtungen im deutschen Hoheitsgebiet statt. Eine demgegenüber auf dem Territorium von Drittstaaten stattfindende Gewinnung von Informationen wird häufig stärker auf Einzelfälle zugeschnitten sein und somit eher einer Situation von „effektiver Kontrolle“ über das Individuum gleichkommen können.

C. Völkerrechtliche Regeln zu staatlicher Spionagetätigkeit

37. Das Verhältnis des Völkerrechts zu staatlicher Spionage ist von einer gewissen Ambivalenz gekennzeichnet: Spionage ist weder ausdrücklich erlaubt noch ist sie als solche grundsätzlich verboten. Da das Völkerrecht in seiner Grundstruktur immer noch vom Konsens der Staaten abhängt, gilt die Grundaussage, dass alle staatlichen Tätigkeiten, die nicht ausdrücklich verboten sind, erlaubt sind.[61] Dies bedeutet aber nicht, dass alle Formen der Spionage völkerrechtlich zulässig sind.[62]

38. Was die Zulässigkeit von Spionage an sich betrifft, so ist zwischen der Spionage in Friedenszeiten und Aktivitäten der Spionage im Zusammenhang mit einem bewaffneten Konflikt zu unterscheiden. Nur für den letzteren Fall, die sog. „Kriegsspionage“ hält das Völkerrecht Regeln vor, die sich unmittelbar mit den Handlungen von Spionen beschäftigen. Da im vorliegenden Kontext nach ganz überwiegender Auffassung kein bewaffneter Konflikt einschlägig ist (und es auch im Rechtssinn keinen globalen „Krieg den Terrorismus“ gibt), muss auf diese in der Haager Landkriegsordnung sowie dem Ersten Zusatzprotokoll zu den Genfer Konventionen niedergelegten Regeln hier nicht weiter eingegangen werden.[63]

39. Für die Spionage in Friedenszeiten gibt es keine allgemeinen völkerrechtlichen Regeln. Aus ihrer Abwesenheit wird, wie soeben schon bemerkt, überwiegend der Schluss gezogen, dass Spionage im Völkerrecht weder erlaubt noch verboten ist. Zugleich ist es völkergewohnheitsrechtlich anerkannt, dass Spione sich nach dem jeweiligen nationalen

---

[61] Auch als das „Lotus-Prinzip” bezeichnet: StIGH, *The Case of the S.S. Lotus, Frankreich/Türkei*, Series A, No. 10, 27.

[62] Vgl. allgemein Dieter Fleck, Individual and State Responsibility for Intelligence Gathering, *Michigan Journal of International Law* 28 (2007), S. 687-709 (688); Christian Schaller, Spies, in: Rüdiger Wolfrum (Hrsg.), *Max Planck Encyclopedia of Public International Law*, 3. Aufl, Oxford 2012, abrufbar unter www.mpepil.com.

[63] Vgl. Art. 46 des Zusatzprotokoll vom 8. Juni 1977 zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte (Protokoll I), BGBl. 1990 II, S. 1550. Die ersten völkerrechtlich verbindlichen Regeln für diesen Bereich wurden in der Haager Landkriegsordnung von 1907 niedergelegt: Anlage zum IV. Haager Abkommen betreffend die Gesetze und Gebräuche des Landkrieges vom 18. Oktober 1907, RGBl. 1910, S. 375, Art. 29-31.

Recht eines Staates strafbar machen können (wie z.B. in Deutschland gemäß § 99 StGB).[64] Durch ihre Taten lösen sie allerdings keine Staatenverantwortlichkeit aus, d.h., dass die Spionage im zwischenstaatlichen Verhältnis keine rechtswidrige Handlung darstellt.[65] Zugleich ist es den Staaten aber verwehrt, für die Akte von Spionen die Regeln der Immunität für das Handeln staatlicher Hoheitsträger in Anspruch zu nehmen.[66] Der Grund für diese Nichteinräumung von Immunität *ratione materiae* wird in der fehlenden Zustimmung des Forumsstaates zu der Tätigkeit der Spionage gesehen.[67] Dies impliziert wiederum, dass eine vorhandene Zustimmung des Forumsstaates zum Aufenthalt von Mitarbeitern eines fremden Geheimdienstes auch dazu führen kann, dass der diese Mitarbeiter entsendende Staat sich gegenüber Strafverfolgungsmaßnahmen auf die Immunität berufen kann. Allerdings ginge es in einem solchen Szenario wohl auch nicht mehr um den Bereich der klassischen zwischenstaatlichen Spionage – dafür wird wohl kaum eine Zustimmung vorliegen, sondern dann vielmehr um andere Formen der Datenerhebung, z.B. gegenüber der Bevölkerung des betroffenen Staates.

40. Eine Ausnahme von der grundsätzlichen Ausnahme von Spionagetätigkeiten aus dem Anwendungsbereich der Regeln über die Immunität *ratione materiae* gilt ferner, soweit es sich bei den Spionen um diplomatisches oder konsularisches Personal mit entsprechenden Immunitäten nach den Wiener Übereinkommen über diplomatische und konsularische Beziehungen[68] handelt.[69] Zwar verhalten sich Diplomaten, die Spionagetätigkeiten begehen, rechtswidrig und lösen damit auch einen Verstoß ihres Staates gegen das Diplomatenrecht aus, da die Informationsbeschaffung nach Art. 3 Abs. 1 d) WÜD nur mit rechtmäßigen Mitteln geschehen darf.[70] Gemäß Art. 41 Abs. 1 S. 1 WÜD sind alle Personen, die Vorrechte und Immunitäten nach dem WÜD genießen, unbeschadet dessen verpflichtet, die Gesetze und andere Rechtsvorschriften des Empfangsstaates zu beachten. Sie sind ferner nach Art. 41 Abs. 1 S. 2 WÜD verpflichtet, sich nicht in die inneren Angelegenheiten des Empfangsstaates einzumischen. Gemäß Art. 41 Abs. 3 WÜD dürfen auch die Räumlichkeiten der Mission nur zu den Zwecken des Abkommens benutzt werden, was eine Verwendung für Zwecke der Spionage ausschließt. Verstoßen Diplomaten gegen diese Bestimmungen, berechtigt dies jedoch nicht zum Entzug der diplomatischen Immunität, die *ratione personae* gilt. Dem Empfangsstaat stehen als Reaktion auf Verletzungen des Diplomatenrechts nur die spezifischen Sanktionen dieses Rechtsgebiets zur Verfügung, insbesondere die Erklärung zur *persona non grata* nach Art. 9 Abs. 1 WÜD.[71]

---

[64] Vgl. auch BVerfGE 92, 277 (321) zum Fehlen einer Regel des allgemeinen Völkerrechts i.S.d. Art. 25 GG, die sich als Rechtfertigungsgrund für Akte der Friedensspionage für festgenommen Agenten auswirken würde.

[65] Simon Chesterman, The Spy Who Came in from the Cold War: Intelligence and International Law, *Michigan Journal of International Law* 27 (2006), S. 1071-1130 (1081).

[66] BVerfGE 92, 277 (321); vgl. auch Roman Anatolevich Kolodkin, Second Report on Immunity of State Officials from Foreign Criminal Prosecution, UN Doc. A/CN.4/631 vom 10.6.2010, Rn. 84 f.

[67] Kolodkin, Second Report (Fn. 66), Rn. 85.

[68] Wiener Übereinkommen über diplomatische Beziehungen vom 18.4.1961, BGBl. 1964 II, S. 959; Wiener Übereinkommen über konsularische Beziehungen vom 24.4.1963, BGBl. 1969 II, S. 1585.

[69] BVerfGE 92, 277 (321).

[70] Vgl. schon Joachim Hinz, Spionage, in: Hans-Jürgen Schlochauer (Hrsg.), *Wörterbuch des Völkerrechts*, 2. Aufl., Bd. 3, Berlin 1962, S. 298-300 (300).

[71] Chesterman (Fn. 65), S. 1089.

41. Spionagetätigkeiten können darüber hinaus gegen weitere völkerrechtliche Regeln verstoßen. Insbesondere das völkergewohnheitsrechtlich geltende Interventionsverbot kann hier einschlägig sein.[72] Nach der Rechtsprechung des Internationalen Gerichtshofs (IGH) liegt allerdings dann ein Verstoß gegen diese Norm vor, wenn die Einmischung in die inneren Angelegenheiten einen Zwangscharakter hat. Dieser Zwangscharakter sei das definierende Merkmal einer verbotenen Intervention:

> „Intervention is wrongful when it uses methods of coercion in regard to such choices [*of a political, economic, social and cultural system, HPA*], which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force (...)."[73]

Von einer solchen Zwangswirkung kann bei nachrichtendienstlicher Datenerhebung nicht gesprochen werden. Auch die Tatsache, dass sich die Ausforschungsmaßnahmen auf den innersten Bereich der Willensbildung einer Regierung beziehen, verleiht ihnen keinen Zwangscharakter.[74] An und für sich nicht verbotene Spionage wird nicht dadurch rechtswidrig, dass sie besonders erfolgreich durchgeführt wird.[75] Dessen ungeachtet können nachrichtendienstliche Maßnahmen, so sie über die bloße Informationsbeschaffung hinausgehen, zweifelsohne gegen völkerrechtliche Regeln verstoßen, wenn etwa Maßnahmen der Sabotage getroffen werden und auf unzulässige Art und Weise Hoheitsgewalt über Individuen ausgeübt wird. Dann handelt es sich aber auch nicht mehr um Spionagemaßnahmen im eigentlichen Sinn. Eine Grenze hat in dieser Hinsicht auch der EGMR in dem Verfahren Weber und Saravia gegen Deutschland gekennzeichnet. Der Gerichtshof konnte in dem konkreten Fall der mittels Satelliten durchgeführten Überwachungsmaßnahmen keine Verletzung der argentinischen Souveränität durch die Bundesrepublik erkennen. Entscheidend ist in diesem Kontext der Hinweis, dass es bei der in Rede stehenden Auslandsüberwachung durch den BND nicht um das Anzapfen von „fixed telephone lines" ging, sondern vielmehr um Satelliten- und Funkverbindungen.[76] Dieser Klarstellung lässt sich entnehmen, dass z.B. eine Manipulation eines zentralen Internetknotenpunkts in einem Staat durchaus der Charakter einer Souveränitätsverletzung zukommen kann.

D. Können Abkommen Deutschlands mit einem oder mehreren Staaten der sog. „Five Eyes" Erhebung, Speicherung auf Vorrat und Austausch von Daten legitimieren?

---

[72] Vgl. Wewer/Thienel (Fn. 41), S. 31; Talmon (Fn. 22).

[73] IGH, *Armed Activities in and against Nicaragua, Nicaragua v. United States*, Merits, Judgment of 14 June 1986, ICJ Rep. 1986, 14, Rn. 205.

[74] Anders aber Peters (Fn. 60).

[75] In diese Richtung lässt sich auch der launige Kommentar von US-Präsident Obama verstehen: „We will not apologize simply because our services may be more effective" (als andere Geheimdienste), Rede zu NSA-Reformen, Washington, 17. Januar 2014, abrufbar unter http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html (zuletzt aufgerufen am 26.5.2014).

[76] EGMR, *Weber und Saravia/Deutschland* (Fn. 23), Rn. 88.

42. Bei der Beantwortung dieser Frage sind verschiedene Aspekte und Dimensionen zu unterscheiden.

I. Die völkerrechtliche Vertragsfreiheit und ihre Grenzen

43. Zunächst gilt der allgemeine Grundsatz der Vertragsfreiheit der Staaten im Völkerrecht.[77] Genauso wie Staaten menschenrechtliche Verträge geschlossen haben, können sie auch ihre Kooperation im nachrichtendienstlichen Bereich durch Verträge weiter ausgestalten (wobei insbesondere in diesem Bereich jeweils genau zu prüfen ist, ob die Staaten einen völkerrechtlich bindenden Vertrag schließen möchten oder nur ein politisch verbindliches „Gentlemen's Agreement").[78]

44. Das Völkerrecht setzt der Vertragsfreiheit der Staaten dabei durch die Kategorie des zwingenden Völkerrechts (*ius cogens*) nach Art. 53, 64 EMRK nur bedingt Grenzen. Die Staaten werden dementsprechend nur durch zentrale Normen der Völkerrechtsordnung vom Abschluss neuer Verträge gehindert. Zu diesen Normen zählen etwa die Verbote von Angriffskrieg, Völkermord, Folter oder Sklaverei. Auch wenn der Schutz der Privatsphäre unstrittig ein wichtiges menschenrechtliches Gut darstellt, handelt es sich dabei ganz eindeutig um keine Norm des *ius cogens*.[79]

45. Von der völkerrechtlichen Dimension zu unterscheiden ist die Frage nach der Vereinbarkeit von solchen Abkommen mit dem jeweiligen nationalen Verfassungsrecht. Die Verfassungsrechtsordnung des GG geht grundsätzlich von einem dualistischen Verhältnis zum Völkerrecht aus, d.h., dass die beiden Rechtskreise des Völkerrechts und des nationalen Rechts voneinander getrennt sind.[80] Es ist dementsprechend möglich, dass sich die Bundesrepublik völkerrechtlich zu etwas verpflichtet, was sie verfassungsrechtlich nicht einlösen kann. Ein Verstoß eines Abkommens zur Erhebung von Daten gegen Art. 10 GG führt somit nicht zu seiner Völkerrechtswidrigkeit. Vielmehr bestimmt Art. 27 S. 1 der Wiener Vertragsrechtskonvention (WVK), dass sich ein Staat nicht auf sein innerstaatliches Recht berufen kann, um die Nichterfüllung eines Vertrages zu rechtfertigen.[81]

46. Eine Ungültigkeit von Verträgen wegen einer fehlenden Übereinstimmung mit innerstaatlichem Verfassungsrecht lässt das Völkerrecht nur in eng umgrenzten Sonderfällen zu, die von Art. 46 WVK näher definiert werden. Wenn die Verletzung einer Vorschrift des innerstaatlichen Rechts offenkundig war und zudem eine Vorschrift von grundlegender Bedeutung betraf, kann sich ein Staat nach Art. 46 Abs. 1 WVK ausnahmsweise darauf berufen, dass seine Zustimmung, durch einen Vertrag gebunden zu sein, unter Verletzung einer Bestimmung seines innerstaatlichen Rechts zustande gekommen ist. Art. 46 Abs. 1 WVK geht dabei aber davon aus, dass es sich um Vorschriften über die Zuständigkeit zum Abschluss von Verträgen gehandelt haben muss. Zudem ist eine Verletzung nur dann offenkundig, wenn sie gemäß Art. 46 Abs. 2 WVK „für jeden Staat, der sich hierbei im Einklang mit der allgemeinen Übung und nach Treu und Glauben verhält, objektiv erkennbar

---

[77] Georg Dahm/Jost Delbrück/Rüdiger Wolfrum, *Völkerrecht*, Bd. I/3, 2. Aufl., Berlin 2002, S. 535.

[78] Vgl. dazu, auf sog. „no spy"-Abkommen bezogen Schmahl (Fn. 41), S. 222.

[79] Für einen Überblick über einschlägige Normen siehe Alexander Orakhelashvili, *Peremptory Norms in International Law*, Oxford 2006, S. 50 ff. Selbst in diesem recht weit gezogenen Katalog von Normen taucht der Schutz der Privatsphäre nicht auf. Vgl. auch Schiedermaier (Fn. 5), S. 61.

[80] BVerfGE 111, 307 (318).

[81] Wiener Übereinkommen über das Recht der Verträge vom 23.5.1969, BGBl. 1985 II, S. 927.

ist". Diesen Vorgaben wird in aller Regel entnommen, dass eine Berufung auf Verstöße gegen materielle Verfassungsrechtssätze nicht zur Ungültigkeit von Verträgen führen kann, da diese in der Praxis vielfach umstritten und auslegungsbedürftig sind.[82] Auch die Frage, unter welchen Umständen ein Vertrag einem innerstaatlichen Zustimmungsverfahren unterzogen werden muss, ist nicht ohne weiteres als so eindeutig anzusehen, dass ein Verstoß gegen innerstaatliches Verfassungsrecht hier eine Berufung auf die Ausnahmeklausel des art. 46 Abs. 1 WVK erlauben würde.[83] In keinem Fall würde sich aus einem Verstoß gegen solche erheblichen Normen eine automatische Nichtigkeit des fraglichen Vertrages ergeben. Vielmehr müsste sich der Staat, der einen relevanten Verstoß gegen seine eigene Verfassungsrechtsordnung geltend machen möchte, auf diesen gegenüber seinen Vertragspartnern berufen.

II. Abkommen in Bezug auf die Bundesrepublik Deutschland

47. Im Hinblick auf die Rechtslage in Deutschland zum Untersuchungszeitpunkt wird teilweise die Frage aufgeworfen, ob das Vorgehen ausländischer Nachrichtendienste in Deutschland eine völkerrechtliche Rechtfertigung im Fortgelten einiger zwischen der Bundesrepublik und den Alliierten geschlossenen Vereinbarungen aus der Zeit vor der Wiedervereinigung finden würde.[84]

48. Die Bundesregierung hat sich auf den Standpunkt gestellt, dass mit der Vereinigung Deutschlands am 3. Oktober 1990 und durch das Inkrafttreten des Zwei-plus-Vier-Vertrages am 15. März 1991 keine alliierten Vorbehaltsrechte mehr gelten. Art. 7 Abs. 1 S. 1 des Zwei-plus-Vier-Vertrages bestimmt, dass die vier Mächte „hiermit ihre Rechte und Verantwortlichkeiten in Bezug auf Berlin und Deutschland als Ganzes" beenden.[85] Art. 7 Abs. 1 S. 2 des Zwei-plus-Vier-Vertrages besagt weiter, dass „als Ergebnis ... die entsprechenden, damit zusammenhängenden vierseitigen Vereinbarungen, Beschlüsse und Praktiken beendet" werden. Obwohl insoweit nur von „vierseitigen" Vereinbarungen die Rede ist, hält die Bundesregierung zusammenfassend fest: „Es gibt keine völkerrechtlichen Vereinbarungen mit den USA, nach denen US-Stellen Daten in Deutschland erheben oder ausleiten können."[86]

49. Bis zum Sommer 2013 galten zumindest Verwaltungsvereinbarungen zwischen der Bundesrepublik Deutschland und den drei Westalliierten weiter, die 1968 im Kontext der sog. „G10-Gesetzgebung" abgeschlossen worden. Nach diesen Abkommen konnten die Alliierten unter gewissen Voraussetzungen deutsche Nachrichtendienste um Überwachungsmaßnahmen ersuchen.[87] Diese Verwaltungsvereinbarungen sind laut der

---

[82] Vgl. zu diesen Fragen die Kommentierung des Art. 46 WVK von Michael Bothe, in: Olivier Corten/Pierre Klein (Hrsg.), *The Vienna Convention on the Law of Treaties – A Commentary*, Bd. II, Oxford 2011, S. 1090-1099.

[83] Zu den Unterschieden hinsichtlich der Zustimmungsbedürftigkeit von Verträgen in verschiedenen innerstaatlichen Rechtsordnungen siehe Bothe (Fn. 82), S. 1095 ff.

[84] Vgl. Dieter Deiseroth, Nachrichtendienstliche Überwachung durch US-Stellen in Deutschland – Rechtspolitischer Handlungsbedarf?, *ZRP* 2013, S. 194-198; Joachim Wolf, Der rechtliche Nebel der deutsch-amerikanischen „NSA-Abhöraffäre", *JZ* 2013, S. 1039-1046.

[85] Vertrag über die abschließende Regelung in Bezug auf Deutschland vom 12.9.1990, BGBl. 1990 II, S. 1317.

[86] BT.-Drs. 17/14560, S. 12.

[87] Das Verwaltungsabkommen mit dem Vereinigten Königreich ist abgedruckt in: Josef Foschepoth, *Überwachtes Deutschland – Post- und Telefonüberwachung in der alten Bundesrepublik*, 3. Aufl., Göttingen 2013, S. 298-301 (Dokument 18c).

Bundesregierung im August 2013 im jeweils beiderseitigen Einvernehmen aufgehoben worden. Zudem sei seit der Wiedervereinigung von ihnen kein Gebrauch mehr gemacht worden.[88] Da diese Abkommen keine Befugnis zu eigenständigen Handlungen der Alliierten in Deutschland vermittelt haben, müsste die Bundesregierung auch in einer Position sein, zu dieser Frage zutreffend Auskunft zu geben.

50. Weiterhin in Kraft ist das Zusatzabkommen vom 3. August 1959 zum NATO-Truppenstatut (im Folgenden: „Zusatzabkommen").[89] Dieses Abkommen sieht auch die Möglichkeit zur Erhebung von gewissen nachrichtendienstlichen Informationen vor. Diese erstrecken sich nach Art. 53 Abs. 1 auf eine Ermächtigung zur Vornahme der erforderlichen Maßnahmen auf ausländischen Truppen zur ausschließlichen Benutzung überlassenen Liegenschaften. Nach Art. 60 können zudem Fernmeldeanlagen und –dienste betrieben werden, soweit dies für militärische Zwecke erforderlich ist. Art. 3 sieht zudem die Möglichkeit vor, mit deutschen Stellen zusammenzuarbeiten, was nach Art. 3 Abs. 2 (a) insbesondere auch den Austausch von Nachrichten beinhaltet.

51. Die Frage, zu was diese Bestimmungen ermächtigen, ist nach den allgemeinen, in Art. 31 und 32 WVK niedergelegten Regeln zur Auslegung völkerrechtlicher Verträge zu bestimmen, die insoweit auch Völkergewohnheitsrecht darstellen und hier dementsprechend auf ein älteres Übereinkommen Anwendung finden.[90] Damit ist nicht nur der Wortlaut der einzelnen Vertragsbestimmung maßgeblich, sondern auch ihr Ziel und Zweck, ebenso wie ihre systematische Stellung im Kontext des Vertragswerkes.[91]

52. Das Zusatzabkommen ist dementsprechend im engen Zusammenhang mit dem NATO-Truppenstatut zu lesen, welches in Art. II erfordert, dass eine Truppe und ihr ziviles Gefolge, ihre Mitglieder und deren Angehörige das Recht des jeweiligen Aufnahmestaates zu beachten haben.[92] Jedenfalls gebietet es eine an Sinn und Zweck orientierte Auslegung des Vertrages, die den Alliierten hier eingeräumten Befugnisse nur so weit zu verstehen, wie es zum Schutz ihrer Truppen in der Bundesrepublik erforderlich ist.

53. Dies gilt, *mutatis mutandis*, auch für den ebenfalls weiter in Kraft befindlichen sog. „Truppenvertrag" von 1954.[93] In diesem Vertrag heißt es, dass die deutschen Behörden und die Behörden der ausländischen Streitkräfte in vollem Umfang zusammenarbeiten und sich gegenseitig bei der Förderung und Wahrung der Sicherheit der Bundesrepublik und der beteiligten Mächte sowie der Sicherheit der im Bundesgebiet stationierten Streitkräfte und deren Mitglieder sowie ihres Eigentums unterstützen, Art. 4 Abs. 1. Diese Zusammenarbeit soll sich nach Art. 4 Abs. 2 des Vertrages, „in Übereinstimmung mit einem zwischen den

---

[88] BT.-Drs. 17/14560, S. 10.

[89] Zusatzabkommen zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen vom 3. August 1959, BGBl. 1961 II, S. 1218.

[90] Vgl. insoweit Richard Gardiner, *Treaty Interpretation*, Oxford 2008, S. 12 f.

[91] Zur Bedeutung der einzelnen Auslegungsmethoden im Rahmen der allgemeinen Auslegungsregel des Art. 31 WVK siehe Mark E. Villiger, The Rules on Interpretation: Misgivings, Misunderstandings, Miscarriage? The Crucible Intended by the International Law Commission, in: Enzo Cannizaro (Hrsg.), *The Law of Treaties Beyond the Vienna Convention*, Oxford 2011, S. 105-122 (108-113).

[92] Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen vom 3. August 1959, BGBl. 1961 II, S. 1183.

[93] Vertrag über die Rechte und Pflichten ausländischer Streitkräfte und ihrer Mitglieder in der Bundesrepublik Deutschland, BGBl. 1954 II, S. 78.

zuständigen Behörden zu treffenden Einvernehmen, auf die Sammlung und den Austausch sowie auf den Schutz der Sicherheit aller einschlägigen Nachrichten" beziehen.

54. Auch wenn diese Bestimmungen denkbar weit formuliert sind[94], sind sie auf den „Deutschlandvertrag" von 1954 bezogen. Dieser ist auf die Gestaltung der deutschen Sondersituation ausgerichtet, wie Formulierungen in der Präambel zu entnehmen ist. Danach bleibt es ein „grundlegendes und gemeinsames Ziel der Unterzeichnerstaaten, ... die Wiederherstellung eines völlig freien und vereinten Deutschlands" zu erreichen. Die alliierten Mächte seien entschlossen, „nur die besonderen Rechte aufrechtzuerhalten, deren Beibehaltung im Hinblick auf die Besonderheiten der internationalen Lage Deutschlands im gemeinsamen Interesse der Unterzeichnerstaaten erforderlich ist."[95] Sowohl das Zusatzabkommen als auch der Truppenvertrag stehen mithin in einem sehr spezifischen Kontext. Die Verträge dürfen jedenfalls nicht so ausgelegt werden, als würde durch sie ein unbegrenztes Recht zur nachrichtendienstlichen Tätigkeit fremder Dienste in der Bundesrepublik gewährt.

55. Zusammenfassend sind demnach auch für den Zeitraum vor dem Jahre 2013 keine bilateralen oder speziell auf Deutschland bezogenen multilateralen Vertragswerke bekannt, welche die Erhebung, Speicherung auf Vorrat und den Austausch von Daten mit einem oder mehreren Staaten der sog. „Five Eyes" legitimieren würden.

56. Zur Existenz von geheimen Abkommen kann keine Aussage getroffen werden. Geheimverträge sind im Völkerrecht nicht grundsätzlich verboten.[96] Nach Art. 102 der UN-Charta soll es aber nicht möglich sein, sich vor Organen der Vereinten Nationen auf sie zu berufen. Dies würde im Rahmen eines etwaigen Verfahrens vor dem Internationalen Gerichtshof dazu führen, dass sich ein Staat der „Five Eyes" auf solche geheimen Abkommen nicht berufen könnte.[97] Geheime Abkommen würden dementsprechend auch vor dem UN-Menschenrechtsausschuss keine Gültigkeit in Anspruch nehmen können.

E. Unionsrechtliche Normen zur Erhebung, Speicherung auf Vorrat, Auswertung und Austausch von Daten

I. Regeln auf Ebene des Primärrechts

57. Das Unionsrecht enthält eine Reihe von Regeln zum Datenschutz und zum Schutz der Privatsphäre auf den Ebenen des Primär- und Sekundärrechts. Art. 16 Abs. 1 AEUV bestimmt, dass jede Person das Recht auf Schutz der sie betreffenden Daten hat. Diese Norm bezieht sich jedoch nur auf den Anwendungsbereich des Unionsrechts, was durch die in Art. 16 Abs.

---

[94] Wolf (Fn. 84), S. 1043.

[95] Vertrag über die Beziehungen zwischen der Bundesrepublik Deutschland und den Drei Mächten, BGBl. 1954 II, S. 61.

[96] Art. 18 der Völkerbundsatzung war weitreichender als Art. 102 UN-Charta, indem er bestimmte, dass ohne Registrierung kein Vertrag bindend sein solle. In der Praxis des Völkerbundes führte die Bestimmung aber zu vielen Unstimmigkeiten, weswegen Art. 102 UN-Charta weniger scharf formuliert wurde. Vgl. m.w.N. Ernst Martens, Art. 102, Rn. 43, in: Bruno Simma/Daniel-Erasmus Khan/Georg Nolte/Andreas Paulus (Hrsg.), *The Charter of the United Nations – A Commentary*, 3. Aufl., Oxford 2012.

[97] Zumindest, wenn ein Staat die Nicht-Registrierung rügt, vgl. Martens (Fn. 96), Art. 102, Rn. 56 mit Beispielen aus der IGH-Rechtsprechung, in denen geheime Abkommen vor dem IGH erwähnt wurden.

2 AEUV normierte Rechtssetzungskompetenz für Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten die in den Anwendungsbereich des Unionsrechts fallen, unterstrichen wird. Gegenüber der Rechtslage vor Inkrafttreten des Vertrags von Lissabon ist die Zuständigkeit der EU auf diesem Bereich gleichwohl erheblich ausgedehnt worden, da die vorher vorhandene Akzessorietät von Regelungen des Datenschutzes zur Binnenmarktkompetenz aufgehoben wurde.[98] Nunmehr entfaltet sie auch Wirkung, wenn es z.B. um Maßnahmen auf dem Gebiet der polizeilichen und justiziellen Zusammenarbeit geht.

58. In diesem Zusammenhang ist allerdings zu berücksichtigen, dass gemäß Art. 4 Abs. 2 S. 3 EUV die nationale Sicherheit weiterhin in die alleinige Verantwortung der Mitgliedstaaten fällt. Diese Bestimmung stellt zunächst eine Präzisierung der allgemeinen Achtung der nationalen Identität der Mitgliedstaaten (Art. 4 Abs. 2 S. 1 EUV) und der Schutzfunktion des Staates für die nationale Sicherheit (Art. 4 Abs. 2 S. 2 EUV) dar. Damit fallen nicht alle staatlichen Maßnahmen, die für sich in Anspruch nehmen, im Namen der nationalen Sicherheit vorgenommen zu werden, aus dem Anwendungsbereich des Unionsrechts heraus.[99] Vielmehr müssen sich mitgliedstaatliche Maßnahmen zum Schutz der nationalen Sicherheit auch an den Vorgaben des Unionsrechts messen lassen, wenn sie im Anwendungsbereich des Unionsrechts vorgenommen werden.[100]

59. Entsprechendes gilt auch für die Verbürgungen des Schutzes der Privatsphäre und des Schutzes personenbezogener Daten in Art. 7 und 8 der Grundrechtecharta. Hier bestimmt sich der Anwendungsbereich nach Art. 51 Abs. 1 GrCh, wonach die Bestimmungen für die Organe, Einrichtungen und sonstigen Stellen der Union gelten sowie für die Mitgliedstaaten „ausschließlich bei der Durchführung des Rechts der Union". Auch wenn der EuGH dies jüngst sehr weitreichend ausgelegt hat[101], ist nicht ersichtlich, dass das Vereinigte Königreich im Rahmen seines Tempora-Programms Unionsrecht durchführen würde. So ist daran festzuhalten, dass der Anwendungsbereich der Unionsgrundrechte im Ergebnis durch die Reichweite der unionsrechtlichen Sekundärrechtssetzung determiniert wird.[102]

60. Unabhängig davon ergibt sich durch das Protokoll Nr. 30 zum Vertrag von Lissabon – welches eine Klarstellung hinsichtlich der Wirkungen der Grundrechte-Charta für Polen und das Vereinigte Königreich vornimmt – keine Ausnahme des Vereinigten Königreichs vom allgemeinen Schutzstandard der europäischen Grundrechte. Vielmehr wird durch das Protokoll nur bekräftigt, dass durch das Verbindlichwerden der Charta keine Ausweitung der Zuständigkeit des EuGH erfolgt und sich insbesondere aus dem Vierten Titel der Grundrechte-Charta, der vor allem soziale Grundrechte enthält, keine neuen Verpflichtungen ergeben. Jedenfalls bleiben die schon in der Rechtsprechung des EuGH als allgemeine Rechtsgrundsätze anerkannten Grundrechte unberührt (was auf den Schutz der Privatheit

---

[98] Thorsten Kingreen, in: Christian Calliess/Matthias Ruffert (Hrsg.), *EUV/AEUV-Kommentar*, 4. Aufl., München 2011, Art. 16 AEUV, Rn. 5.

[99] EuGH, *Kommission/Italien*, Rs. C-387/05, Urteil vom 15.12.2009, Slg. 2009, I-11831, Rn. 45; EuGH, *ZZ/Secretary of State for the Home Department*, Rs. C-300/11, Urteil vom 4.6.2013, Rn. 38.

[100] Siehe auch Wewer/Thienel (Fn. 41), S. 33.

[101] EuGH, *Åkerberg Fransson/Schweden*, Rs. C-617/10, Urteil vom 26. Februar 2013, Rn. 16 ff. = NJW 2013, 1415.

[102] Thorsten Kingreen, in: Calliess/Ruffert (Fn. 98), Art. 8 GrCH, Rn. 6.

zutrifft), ebenso wie Rechte, welche im Primärrecht eine eigenständige Basis haben (wie dies bei Art. 16 AEUV für den Datenschutz der Fall ist).[103]

61. Die vor kurzem ergangene Entscheidung des EuGH zur sog. „Vorratsdatenspeicherung" unterstreicht dabei den Stellenwert, den der Schutz der Privatsphäre und persönlicher Daten in der Unionsrechtsordnung ganz grundsätzlich einnehmen.[104] Für den vorliegenden Kontext sind die folgenden Aussagen des Gerichtshofs von Belang:

    - Auch aus der Erhebung von sog. „Metadaten" – d.h. Daten, die nicht die Inhalte der Kommunikation betreffen – können sehr genaue Rückschlüsse auf das Privatleben von Personen gezogen werden.[105]
    - Für die Feststellung eines Eingriffs in das Grundrecht auf Achtung des Privatlebens kommt es nicht darauf an, ob die betreffenden Informationen sensiblen Charakter haben oder ob die Betroffenen durch die Maßnahme Nachteile erleiden.[106]
    - Der Zugang nationaler Behörden zu den gespeicherten Daten stellt einen separaten Eingriff in die betroffenen Grundrechte dar.[107]
    - Das große Ausmaß der Vorratsspeicherung führt dazu, dass es sich um einen besonders schwerwiegenden Eingriff handelt, da sich für die Bürgerinnen und Bürger der Eindruck ergeben kann, „dass ihr Privatleben Gegenstand einer ständigen Überwachung" ist.[108]
    - Auch wenn der Eingriff besonders schwerwiegend ist, wird nicht der Wesensgehalt der Grundrechte aus Art. 7, 8 GrCh missachtet, da die Inhalte der Kommunikation nicht zur Kenntnis genommen werden und es außerdem Bestimmungen zum Datenschutz hinsichtlich des gewonnenen Materials gebe.[109]
    - Die Bekämpfung schwerer Kriminalität ist eine dem Gemeinwohl dienende Zielsetzung, welche Eingriffe in Art. 7, 8 GrCH rechtfertigen kann.[110] In diesem Zusammenhang hebt der Gerichtshof hervor, dass nach Art. 6 GrCH „jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat".[111]
    - Um eine verhältnismäßige Beschränkung darzustellen, muss eine fragliche Unionsrechtsregelung „klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahmen vorsehen und Mindestanforderungen aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer

---

[103] Schiedermaier (Fn. 5), S. 337 f.; Schmahl (Fn. 41), S. 223; allgemein zum "Opt out" Hans D. Jarass, *Charta der Grundrechte der Europäischen Union – Kommentar*, 2. Aufl., München 2013, Art. 51, Rn. 33.

[104] EuGH, *Digital Rights Ireland/Minister for Communications, Marine and Natural Ressources u.a.*, Urteil vom 8. April 2014, verb. Rs. C-293/12 und C-594/12.

[105] EuGH, *Digital Rights* (Fn. 104), Rn. 27.

[106] EuGH, *Digital Rights* (Fn. 104), Rn. 33.

[107] EuGH, *Digital Rights* (Fn. 104), Rn. 35.

[108] EuGH, *Digital Rights* (Fn. 104), Rn. 37.

[109] EuGH, *Digital Rights* (Fn. 104), Rn. 39, 40.

[110] EuGH, *Digital Rights* (Fn. 104), Rn. 41-44.

[111] EuGH, *Digital Rights* (Fn. 104), Rn. 42.

personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen."[112]

62. Auch wenn das Unionsrecht auf nachrichtendienstliche Datenerhebung keine unmittelbare Anwendung findet, verdeutlicht das Urteil des EuGH zur Vorratsdatenspeicherung die grundsätzliche Unvereinbarkeit einer anlasslosen und flächendeckenden Erfassung von Telekommunikationsdaten mit Grundwerten des Unionsrechts. Bemerkenswert ist auch die zu beobachtende argumentative Konvergenz sowohl mit der nationalen Verfassungsrechtsprechung – konkret des Bundesverfassungsgerichts – als auch mit der Judikatur des EGMR.[113]

II. Regeln auf Ebene des Sekundärrechts

63. Auf der Ebene des Sekundärrechts gibt es weitreichende unionsrechtliche Vorgaben für die Erhebung, Speicherung, Verarbeitung und Weitergabe von Daten. In den entsprechenden Sekundärrechtsakten findet sich jedoch regelmäßig eine Bereichsausnahme für die hier interessierenden Formen der nachrichtendienstlichen Informationserhebung.[114] Dementsprechend ist die nachrichtendienstliche Tätigkeit zunächst nicht vom Anwendungsbereich der RiL 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[115] und von RiL 2002/58/EG (überarbeitet durch RiL 2009/136/EG) über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation[116] umfasst.

64. Ausweichlich ihrer Präambel will die RiL 95/46/EG eine Konkretisierung und Erweiterung der im Europarat-Abkommen von 1981 enthaltenen Grundsätze darstellen.[117] Grundsätzlich gilt die Richtlinie gemäß ihres Art. 3 Abs. 1 für die „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht-automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen." Nach Art. 3 Abs. 2, 1. Spiegelstrich findet die Richtlinie aber „auf keinen Fall" auf Verarbeitungen Anwendung, welche die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt" Anwendung. Art. 1 Abs. 3 der RiL 2002/58/EG enthält eine inhaltsgleiche Klausel. Bei diesen Klauseln handelt es sich um Konkretisierungen von Art. 4 Abs. 2 S. 3 EUV.[118]

65. In Erwägung Nr. 11 zur RiL 2002/58/EG wird die Bedeutung dieser Bereichsausnahme noch näher erläutert:

---

[112] EuGH, *Digital Rights* (Fn. 104), Rn. 54.

[113] Vielfach zitiert der EuGH die maßgebliche EGMR-Rspr., so etwa in EuGH, *Digital Rights* (Fn. 104), Rn. 35, 47, 54, 55; zu den verfassungsrechtlichen Standards in Deutschland siehe BVerfGE 125, 260 (309 ff.).

[114] Wewer/Thienel (Fn. 41), S. 34.

[115] RiL 95/46/EG des Europäischen Parlamentes und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31.

[116] RiL 2002/58/EG (überarbeitet durch RiL 2009/136/EG) über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 201 vom 31.7.2002, S. 37.

[117] RiL 95/46/EG (Fn. 115), Erwägung Nr. 11.

[118] Schmahl (Fn. 41), S. 224.

„Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen, sofern dies erforderlich ist, um einen dieser Zwecke [*der in Art. 1 Abs. 3 der RiL genannten, HPA*] zu erreichen, und sofern dies im Einklang mit der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrecht erfolgt. Diese Maßnahmen müssen sowohl geeignet sein als auch in einem strikt angemessenen Verhältnis zum intendierten Zweck stehen und ferner innerhalb einer demokratischen Gesellschaft notwendig sein…"

Das Bundesverfassungsgericht hat in seiner Entscheidung zur „Antiterror-Datei" bekräftigt, dass es sich in Bezug auf die Datenschutzrichtlinie schon aus Art. 3 Abs. 2 der Richtlinie 95/46/EG ergebe, dass die öffentliche Sicherheit, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich betreffende Datenverarbeitung ausdrücklich aus ihrem Anwendungsbereich ausgenommen sei.[119] Diese Argumentation wird sich auf den nachrichtendienstlichen Bereich übertragen lassen. Für diese kategorische Position ist es in der Literatur im Lichte der NSA- und GCHQ-Enthüllungen kritisiert worden.[120] Die zitierte Erwägung Nr. 11 könnte zwar so gelesen werden, dass der Anwendungsbereich der RiL 2002/58/EG nur insoweit ausgeschlossen sein soll, wie die Vorgaben der EMRK und der entsprechenden Rechtsprechung des EGMR eingehalten werden. Zudem soll die Bereichsausnahme nur gelten, wenn dies für Zwecke der nationalen Sicherheit erforderlich ist, was eine Überprüfung der nationalen Maßnahmen am Maßstab des unionsrechtlichen Verhältnismäßigkeitsprinzips ermöglichen könnte.[121] Allerdings würde eine solche Lesart – auf den Erwägungen der RiL 2002/58/EG basierend – dem insoweit klarer formulierten Art. 1 Abs. 3 der RiL 2002/58/EG widersprechen. Für die RiL 95/46/EG gilt eine ähnliche Erwägung. Eine Eröffnung der Überprüfung von nachrichtendienstlichen Maßnahmen am Maßstab der Verhältnismäßigkeitsprüfung würde letztlich dazu führen, dass Tätigkeiten in diesem Bereich einer umfassenden gerichtlichen Kontrolle unterworfen würden, was der klaren Formulierung der Bereichsausnahme zuwiderläuft. Bis auf weiteres ist mithin daran festzuhalten, dass die Sekundärrechtsakte der Union keine Anwendung auf die Tätigkeit von Nachrichtendiensten finden. Zu diesem Ergebnis kam im Übrigen auch der Nichtständige Ausschuss des Europäischen Parlaments über das Abhörsystem Echelon in seinem 2001 vorgelegten Bericht.[122]

III. Verpflichtung der Mitgliedstaaten auf die Grundwerte der Union

66. Die Erhebung, Verarbeitung und Weitergabe von Daten durch Nachrichtendienste kann – ähnlich wie im Völkerrecht die Friedensspionage – aber in indirekter Form Gegenstand von Regelungen des Unionsrechts werden.

---

[119] BVerfG, 1 BvR 1215/07, Urteil vom 24.4.2013, Rn. 90 = NJW 2013, 1499.

[120] Franz C. Mayer, Mit Europarecht gegen die amerikanischen und britischen Abhörmaßnahmen? Teil 2: GCHQ, *Verfassungsblog* vom 18.11.2013, abrufbar unter http://www.verfassungsblog.de/mit-europarecht-gegen-amerikanischen-und-britischen-abhoeraktionen-teil-2-gchq/ (zuletzt aufgerufen am 25.5.2014); daran angelehnt Schmahl (Fn. 41), S. 224.

[121] Schmahl (Fn. 41), S. 224.

[122] Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON), (2001/2098/INI) vom 11. Juli 2001, Nr. 7.2.1.

67. Die Union gründet sich gemäß Art. 2 S. 1 EUV auf bestimmte Grundwerte, zu denen die Achtung der Menschenwürde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und die Wahrung der Menschenrechte zählen. Eine flächendeckende Überwachungspraxis eines Mitgliedstaates, die nicht die menschenrechtlichen Standards einhält, die der EGMR in seiner Rechtsprechung zu Art. 8 EMRK festgehalten hat, stellt einen Verstoß gegen diese Grundwerte der Union dar – wie die Entscheidung des EuGH zur Vorratsspeicherung jüngst unterstrichen hat.[123] In diesem Zusammenhang ist an das Verfahren nach Art. 7 EUV zu erinnern, welches im Fall einer schwerwiegenden Verletzung der Werte der Union die Möglichkeit der Befassung der Organe der Union mit dieser Praxis vorsieht und bis hin zu einer Einschränkung von Mitgliedschaftsrechten führen kann.[124]

68. Sollte es zudem eine Praxis der Zusammenarbeit zwischen einem Geheimdienst eines Mitgliedstaates und Unternehmen des betreffenden Staates geben, in der auch durch Überwachungsmaßnahmen gewonnene Informationen weitergegeben werden, könnten auch wirtschaftliche Aspekte des Unionsrechts betroffen sein. Zu denken wäre hier etwa an Verstöße gegen die Grundfreiheiten des Unionsrechts, wie etwa der Warenverkehrsfreiheit nach Art. 34 AEUV.[125]

IV. Unionsrechtliche Vorgaben für staatliche Stellen der sog. „five eyes"

69. Das primäre und sekundäre Unionsrecht gilt naturgemäß nur für die Mitgliedstaaten der Europäischen Union. Dementsprechend ist von den sog. „five eyes" nur das Vereinigte Königreich unmittelbar an die unionsrechtlichen Bestimmungen gebunden.

70. Handeln staatliche Stellen der vier anderen Mitglieder der „five eyes" in den Mitgliedstaaten der EU, sind diese Stellen an das Recht der Union gleichwohl genauso gebunden, wie sie auch jeweils das anzuwendende nationale Recht des Forumsstaates zu beachten haben. Diese Verpflichtung ergibt sich dann nicht unmittelbar aus dem Unionsrecht, sondern vielmehr aus der Territorialhoheit der jeweils betroffenen Staaten, in Verbindung mit dem Grundsatz der unmittelbaren Anwendbarkeit des Unionsrechts.[126] Angesichts des eher indirekten Einschlags des Unionsrechts für nachrichtendienstliche Tätigkeiten ergeben sich dadurch aber in der Sache keine relevanten Einschränkungen der Handlungsfreiheit der vier anderen Mitglieder der „five eyes".

71. Allerdings kann das Unionsrecht in noch einer anderen Form indirekt auf die Möglichkeiten einer umfassenden Überwachung durch ausländische Nachrichtendienste Einfluss gewinnen. Das jüngst ergangene Urteil des EuGH im Fall *Google* hat unterstrichen, dass sich auch ausländische Unternehmen sich im Rahmen ihrer Aktivitäten an die europäische Rechtsordnung halten müssen, wenn sie zum Beispiel eine Niederlassung in Mitgliedstaaten der Union unterhalten und hier Werbeflächen vermarkten und verkaufen.[127] Wird nun – wie es vom Europäischen Parlament im letzten Entwurf zu einer neuen

[123] EuGH, *Digital Rights* (Fn. 104).

[124] Vgl. auch Mayer (Fn. 120), der die Frage aufwirft, ob man einen Beitrittskandidaten mit einem so weit ausgebauten Ausspähprogramm in die Union aufnehmen würde und dies verneint.

[125] Für Überlegungen in diese Richtung Mayer (Fn. 120); skeptisch hingegen Wewer/Thienel (Fn. 41), S. 33.

[126] Zur unmittelbaren Anwendbarkeit m.w.N. Matthias Ruffert, in: Calliess/Ruffert (Fn. 98), Art. 1 AEUV, Rn. 25 ff.

[127] EuGH, *Google Spain u.a./ Agencia Española de Protección de Datos (AEPD) u.a.*, Rs. C-131/12, Urteil vom 13.5.2014, Rn. 45-60.

Datenschutzgrundverordnung in Art. 43 a vorgesehen ist[128] – die Möglichkeit der Weitergabe von Daten an staatliche Stellen von Drittstaaten eingeschränkt, so kann sich dies auch auf die Handlungsmöglichkeiten ausländischer Nachrichtendienste auswirken.[129] Die Unternehmen wären dann zwar unter Umständen einem Konflikt zwischen sich widersprechenden Anordnungen US-amerikanischen und europäischen Rechts ausgesetzt.[130] Ein solcher Konfliktfall könnte aber einen wertvollen Anstoß für den transatlantischen Dialog über die einzuhaltenden Datenschutzstandards geben.

V. Das Unionsrecht als Hebel zur Durchsetzung europäischer Standards

72. Mittelbare Bedeutung kann das Unionsrecht zudem als Hebel zur Verteidigung gemeineuropäischer Standards gewinnen. Dies betrifft vor allem eine Suspendierung der Kooperation im Rahmen der Weitergabe von Fluggastdaten sowie von Daten im Rahmen des internationalen Zahlungsverkehrs. In diesem Sinn hat das Europäische Parlament im Oktober 2013 einen Entschließungsantrag beschlossen, wonach das SWIFT-Abkommen aus dem Jahre 2009 ausgesetzt werden soll.[131] Eine weitere Reaktionsmöglichkeit betrifft die sog. Safe Harbour-Absprache. Art. 25 Abs. 1 der RiL 95/46/EG bestimmt, dass die Übermittlung personenbezogener Daten in einen Drittstaat nur dann zulässig ist, wenn in diesem ein angemessenes Datenschutzniveau vorhanden ist. In diesem Kontext wäre es für die Kommission möglich, die Vereinigten Staaten nicht mehr als sicheres Drittland anzusehen, welches ein angemessenes Schutzniveau sichert.[132] An eine solche Maßnahme anknüpfend würden sich auch Handlungsmöglichkeiten für nationale Datenschutzbehörden ergeben, die Weitergabe von Daten in die Vereinigten Staaten zu untersagen (in Deutschland nach § 38 Abs. 5 BDSG).

73. Ob sich allerdings, wie in der Literatur teilweise behauptet[133], das Handlungsermessen der Kommission in dieser Frage auf Null reduziert hat, erscheint fraglich. Ähnlich wie im Bereich der EMRK können sich auch aus den Unionsgrundrechten Schutzpflichten ergeben. Allerdings hängt die Aktivierung dieser Schutzpflichten von der Eröffnung des Anwendungsbereichs des Unionsrechts ab. Durch die Bereichsausnahmen für die nationale Sicherheit sowohl im Primär- wie auch im Sekundärrecht ist es mithin schwierig, hier rechtlich verbindliche Schutzpflichten zu begründen. Die Union verfügt bei der Umsetzung von Schutzaufgaben jedenfalls über einen weiten Einschätzungs- und Gestaltungsspielraum. Wie im deutschen Verfassungsrecht wird dieser auch für die Unionsorgane im Bereich des auswärtigen

---

[128] Eine inoffizielle konsoldierte Fassung der geplanten Datenschutzgrundverordnung ist abrufbar auf der Website des Verhandlungsführers des Europäischen Parlaments, http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/alles-wichtige-zur-datenschutzreform.html (zuletzt aufgerufen am 23.5.2014).

[129] Dazu Franz C. Mayer, Mit Europarecht gegen die amerikanischen und britischen Abhöraktionen? Teil 1: NSA, *Verfassungsblog* vom 18.11.2013, abrufbar unter http://www.verfassungsblog.de/mit-europarecht-gegen-amerikanischen-und-britischen-abhoeraktionen-teil-2-gchq/ (zuletzt aufgerufen am 25.5.2014).

[130] Vgl. auch Kuner (Fn. 2), S. 181.

[131] Entschließungsantrag des Europäischen Parlaments zur Aussetzung des SWIFT-Abkommens infolge der Überwachungsmaßnahmen der NSA, 16.10.2013, 2013/2831(RSP).

[132] Vgl. zuletzt in Bezug auf die Vereinigten Staaten die Entscheidung der Kommission 2000/520/EG, OJ L 215, 25/08/2000, S. 7–47.

[133] Schmahl (Fn. 41), S. 226.

Handelns größer sein als bei Zusammenhängen, die nur unionsinterne Sachverhalte betreffen.[134]

F. Möglichkeiten des (individuellen) Rechtsschutzes

74. Betroffene können gemäß Art. 34 EMRK eine Individualbeschwerde vor dem Europäischen Gerichtshof für Menschenrechte erheben. Diese kann sich direkt gegen das Vereinigte Königreich als Mitglied der „five eyes" wenden, wie auch gegen andere Vertragsparteien der EMRK, denen die Betroffenen eine Verletzung ihrer Schutzpflichten nach der Konvention vorwerfen können. In einer anhängigen Beschwerde gegen das Vereinigte Königreich[135] wird der Gerichtshof die Gelegenheit haben, auch die Fragen der Zulässigkeit einer solchen Beschwerde näher zu klären. So hat die 4. Sektion des Gerichtshofs den Parteien in diesem Fall bereits Fragen zur Opfereigenschaft der Beschwerdeführer (nach Art. 34 EMRK) und zur Erschöpfung des innerstaatlichen Rechtsweges (Art. 35 Abs. 1 EMRK) vorgelegt. Im Lichte der bisherigen Rechtsprechung des Gerichtshofs erscheint es als wahrscheinlich, dass der EGMR die Opfereigenschaft bei der Existenz eines quasi allumfassenden Überwachungssystems, wie es „Tempora" darstellt, bejahen wird, da er in seinen früheren Entscheidungen bereits festgehalten hat, dass bereits die Existenz eines Überwachungssystems einen Eingriff in das Recht auf Privatsphäre darstellen kann.[136] Da für den Einzelnen zudem die Rechtsschutzmöglichkeiten im innerstaatlichen Bereich gegen geheim gehaltene Überwachungsprogramme häufig eher theoretischer Natur sind, ist ebenfalls nicht zu erwarten, dass Individualbeschwerdeverfahren in diesem Zusammenhang an fehlenden Klagen vor den innerstaatlichen Gerichten scheitern werden. Der Gerichtshof hat in seiner Rechtsprechung wiederholt darauf hingewiesen, dass die Erschöpfung des innerstaatlichen Rechtsweges nur dann vorausgesetzt werden kann, wenn es sich um praktisch wirksame Rechtsschutzmöglichkeiten handelt.[137]

75. Verstöße gegen den IPbpR können von betroffenen Individuen im Wege der Individualbeschwerde vor dem MRA geltend gemacht werden. Voraussetzung dafür ist allerdings, dass der Staat, gegen den sich die Beschwerde richten soll, auch Vertragspartei des 1. Zusatzprotokolls zum IPbpR ist. Von den Staaten der sog. „five eyes" trifft dies auf Australien, Kanada und Neuseeland zu. Auch die Bundesrepublik hat sich dem Individualbeschwerdeverfahren angeschlossen.

76. Auch wenn es sich nicht durchweg um Verfahren des individuellen Rechtsschutzes handelt, ist hier ergänzend auf eine Reihe von Möglichkeiten hinzuweisen, mit denen die Dimensionen nachrichtendienstlicher Aktivitäten im Verhältnis zu Staaten der sog. „five eyes" Gegenstand von Gerichtsverfahren werden könnten:

    - Der Europäische Gerichtshof für Menschenrechte könnte im Wege des Staatenberichtsverfahrens nach Art. 33 EMRK befasst werden.

---

[134] Für das deutsche Verfassungsrecht vgl. BVerfGE 68, 1 (87).

[135] Vgl. die anhängige Beschwerde Nr. 58170/13 – *Big Brother Watch u.a./Vereinigtes Königreich*, in der der Gerichtshof am 9.1.2014 Fragen an die Parteien gerichtet hat.

[136] Siehe die Entscheidungen in den Fällen *Weber und Saravia/Deutschland* (Fn. 23) und *Liberty u.a./Vereinigtes Königreich* (Fn. 23).

[137] Dazu im Überblick Patrick Schäfer, Art. 35, Rn. 22 m.w.N., in: Karpenstein/Mayer (Fn. 17).

- Vor dem Internationalen Gerichtshof können die Vereinigten Staaten nach dem Zusatzprotokoll über das WÜD wegen Verstößen gegen das Diplomatenrecht verklagt werden.[138]
- Das Vereinigte Königreich, Australien und Neuseeland haben sich ebenso wie die Bundesrepublik Deutschland allgemein der Gerichtsbarkeit des IGH mittels Erklärungen nach Art. 36 Abs. 2 IGH-Statut unterworfen.[139]
- Im Hinblick auf alle sog. „five eyes"-Staaten kommt zudem die Inanspruchnahme des Staatenbeschwerdeverfahrens nach Art. 41 Abs. 1 IPbpR in Frage, für das die notwendigen Erklärungen von Australien, Kanada, Neuseeland, dem Vereinigten Königreich und den Vereinigten Staaten abgegeben worden sind.[140]
- Wegen etwaiger Verstöße gegen das Unionsrecht könnte auch vor dem Gerichtshof der Europäischen Union ein Vertragsverletzungsverfahren durch die Bundesrepublik Deutschland gegen das Vereinigte Königreich angestrengt werden, Art. 259 Abs. 1 AEUV. Vorher müsste nach Art. 259 Abs. 2 AEUV die Kommission damit befasst werden.
- Die Auslegung des Unionsrechts könnte zudem aus einem mitgliedstaatlichen Gerichtsverfahren heraus im Wege des Vorabentscheidungsverfahrens nach Art. 267 Abs. 1 AEUV vor den EuGH gebracht werden. Dies könnte sich z.B. durch eine Frage der Auslegung der Bereichsausnahmen in den Datenschutzrichtlinien ergeben.
- Der Vollständigkeit halber erwähnt sei zudem die Untätigkeitsklage nach Art. 265 Abs. 1 AEUV, mit der die Organe der Union sowie die Mitgliedstaaten eine pflichtwidrige Unterlassung einer Beschlussfassung durch das Europäische Parlament, den Europäischen Rat, den Rat, die Kommission oder die Europäische Zentralbank rügen können. Nach Art. 265 Abs. 3 AEUV steht diese Klageart auch natürlichen und juristischen Personen offen, die Beschwerde darüber führen können, dass ein Organ oder eine Einrichtung oder sonstige Stelle der Union es unterlassen hat, einen anderen Akt als eine Empfehlung oder eine Stellungnahem an sie zu richten. Letztere Möglichkeit dürfte im vorliegenden Kontext jedoch kaum relevant sein, weil hier nicht ersichtlich, was für einen Rechtsakt die Unionsorgane an eine betroffene natürliche oder juristische Person zu richten hätten. Ein Mitgliedstaat könnte jedoch z.B. eine Verletzung der ihr zukommenden Schutzpflichten durch die Kommission rügen, sollte diese sich etwa weigern, den Austausch von Daten im Rahmen der „safe harbour"-Absprache einzuschränken. Ob ein solcher Antrag allerdings erfolgversprechend ist, ist im Lichte der obigen Ausführungen zweifelhaft.

---

[138] Wiener Übereinkommen über diplomatische Beziehungen, Fakultativ-Protokoll über die Regelungen von Streitigkeiten vom 18.4.1961, BGBl. 1964 II, S. 1018.

[139] Vgl. die Erklärungen Australiens vom 22.3.2002, Deutschlands vom 1.5.2008, Neuseelands vom 22.9.1977 und des Vereinigten Königreichs vom 5.7.2004, alle abrufbar unter http://www.icj-cij.org/jurisdiction/index.php?p1=5&p2=1&p3=3 (zuletzt aufgerufen am 22.5.2014).

[140] Abrufbar unter https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=iv-4&chapter=4&lang=en (zuletzt aufgerufen am 22.5.2014).

G. Zusammenfassung und Ausblick

77. Zusammenfassend zeigt sich im Völker- und Europarecht eine differenzierte Rechtslage hinsichtlich der nachrichtendienstlichen Erhebung, Speicherung, Verwendung und Weitergabe von Daten. Dieses differenzierte Bild ist dem partiellen Charakter völkerrechtlicher und unionsrechtlicher Regulierung geschuldet. Diese erstreckt sich nicht automatisch auf jede Form staatlichen Handelns. Anders als etwa im deutschen Verfassungsrecht gibt es auch keine Art. 19 Abs. 4 GG vergleichbare Generalklausel, wonach gegen jede Form öffentlichen Handelns ein Rechtsbehelf vorhanden sein muss. Zwar ist das Völkerrecht immer anwendbar, wenn Staaten international handeln – es hält aber nicht in jedem Einzelfall auch Regeln zur rechtlichen Beurteilung ihres Handelns bereit. Das Völkerrecht bleibt insoweit eine fragmentarische Rechtsordnung. Für das Unionsrecht folgt ähnliches aus dem Grundsatz der begrenzten Einzelermächtigung, nach dem die Union nur auf den Gebieten handeln darf, auf denen ihr die Mitgliedstaaten Kompetenzen übertragen hat, Art. 4 Abs. 1 EUV.

78. Gleichwohl setzen sowohl das Völkerrecht als auch das Unionsrecht Maßnahmen der globalen Überwachung, wie sie etwa von NSA und GCHQ im Rahmen der PRISM- und Tempora-Programme vorgenommen werden, Grenzen. Diese ergeben sich vor allem aus menschenrechtlichen Regeln und – zu einem geringeren Grad – aus Regeln des „klassischen", zwischenstaatlichen Völkerrechts, wenn bestimmte Formen der nachrichtendienstlichen Tätigkeit nicht mehr nur in reiner Nachrichtenbeschaffung bestehen.

79. Das internationale Datenschutzrecht, so man von einem solchen Rechtsgebiet überhaupt sprechen möchte, ist demgegenüber weniger ergiebig. Dies erscheint auch in gewisser Weise konsequent: Datenschutzrecht setzt eine regelmäßige Erhebung von Daten in einem geordneten Verfahren voraus. Vorgänge wie „PRISM" oder „Tempora" in die Schablonen dieses Rechtsgebiets pressen zu wollen erscheint wenig erfolgsversprechend. Am ehesten können datenschutzrechtliche Regeln in mittelbarer Form Bedeutung gewinnen, indem sie es Unternehmen der Privatwirtschaft erschweren, auf „Kooperationsangebote" von Nachrichtendiensten zu reagieren. Jedenfalls würden strengere Regeln zur Weitergabe von Daten die betroffenen Unternehmen dazu zwingen, gegenüber ihrer jeweiligen Regierung den wirtschaftlichen Preis für globale Überwachungstätigkeit deutlich zu artikulieren.

80. Das Unionsrecht bietet ebenfalls nur relativ schwache Anknüpfungspunkte, um die besagten Überwachungsmaßnahmen in den Griff zu bekommen. Sein Potential liegt eher darin begründet, dass über unionsrechtliche Instrumente ein Hebel geschaffen werden kann, um europäische Grundwerte gegenüber den Vereinigten Staaten zur Geltung zu bringen. Die Beteiligung des Vereinigten Königreichs an den hier in Rede stehenden Formen der Überwachung zeigt allerdings, dass es auch innerhalb der Union nicht leicht ist, einen Konsens hinsichtlich der Schutzstandards für die Privatsphäre zu begründen.

81. Dies sollte auch bei der weiteren Arbeit an der Konkretisierung universaler Normen, zum Beispiel anknüpfend an die Resolution der Generalversammlung aus dem Jahre 2013, im Auge behalten werden.[141] Die Standards, die für die Auslegung von Art. 17 IPbpR gelten sollen, müssen als universale Standards gedacht werden. Dies wirft zwei Fragen auf: Zum einen ist zu berücksichtigen, dass nachrichtendienstliche Maßnahmen legitimen Zwecken und Zielen dienen können. Bei einer weiteren Stärkung des internationalen Schutzes der Privatsphäre wird es nicht nur um das Verhältnis zwischen amerikanischen Diensten und den

[141] Vgl. oben Fn. 18.

Bürgerinnen und Bürgern westlicher Staaten gehen können. Zum anderen ist das Risiko einzuberechnen, diese erste Überlegung zu ignorieren. Der Glaubwürdigkeit des internationalen Menschenrechtsschutzes wird es nicht zuträglich sein, wenn „Sonderrecht" für bestimmte, hauptsächlich westliche Staaten gesetzt wird, dessen Einhaltung angesichts der Durchsetzungsschwäche der universellen Menschenrechtsnormen im Hinblick auf die Praktiken der Überwachung in anderen Staaten – sowohl durch eigene wie auch fremde Dienste – von vornherein illusorisch ist. Kurzum: insbesondere auf der Ebene des IPbpR ist immer an die Universalisierbarkeit der materiellen Standards zu denken.[142]

82. Außerdem sollte nicht aus den Augen verloren werden, dass auch der BND nach seinen gesetzlichen Grundlagen zu sehr weitreichenden Formen der Auslandsüberwachung ermächtigt ist, auf die nach der Rechtsauffassung der Bundesregierung weder die deutschen Grundrechte noch das „G10-Gesetz" Anwendung findet.[143] Im Kontext des Weber und Saravia-Verfahrens vor dem EGMR hatte die Bundesregierung sich auch auf die Position gestellt, dass die EMRK bei Maßnahmen der Auslandsaufklärung des BND keine Anwendung finde. Die Überwachung des Telekommunikationsverkehrs in Argentinien sollte zudem keinen Eingriff in die argentinische Souveränität darstellen.[144]

83. Auch wenn es im Völkerrecht für die Geltendmachung von (untechnisch gesprochen) Ansprüchen keine „clean hands"-Doktrin gibt[145], gibt es doch den Grundsatz des *venire contra factum proprium*.[146] Wer sich als Staat selbst an weitreichenden Programmen der nachrichtendienstlichen Überwachung beteiligt, kann dies kaum glaubwürdig kritisieren. Dazu kommt, dass sich durch Kooperationen im nachrichtendienstlichen Bereich auch eine Haftung der Bundesrepublik für Beihilfe zu Völkerrechtsverstößen ergeben kann.[147] Dabei kommt es entscheidend auf die Zwecke an, für die weitergegebene Daten und Informationen verwandt werden. Die Diskussion um die sog. „gezielten Tötungen" unterstreicht die Tragweite der hiermit verbundenen Probleme.

---

[142] In diese Richtung auch Markus Kotzur, Datenschutz als Menschenrecht?, *ZRP* 2013, S. 216-217 (217).

[143] Vgl. die Stellungnahme von Matthias Bäcker für den Untersuchungsausschuss, MAT A, SV 2-3, zu A-Drs. 54, abrufbar unter http://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848 (zuletzt aufgerufen am 23.5.2014).

[144] EGMR, *Weber und Saravia* (Fn. 23), Rn. 66, 81.

[145] Vgl. Stephen M. Schwebel, Clean Hands, Principle, in: Rüdiger Wolfrum (Hrsg.), *Max Planck Encyclopedia of Public International Law*, Bd. II, 3. Aufl, Oxford 2012, S. 232-235.

[146] Alfred Verdross/Bruno Simma, *Universelles Völkerrecht*, 3. Aufl., Berlin 1984, § 62.

[147] Dazu Aust (Fn. 40).