Erik Tuchtfeld[*]

Das Recht auf Schutz der Privatsphäre im Cyberspace

Abstract

Der Beitrag stellt das Mehrebenensystem des internationalen Menschenrechtsschutzes am Beispiel des Rechts auf Schutz der Privatsphäre im Cyberspace dar. Neben Normen des globalen Menschenrechtsschutzes werden Besonderheiten des regionalen Menschenrechtsschutzes anhand der EMRK sowie des Unionsrechts behandelt. Ein Schwerpunkt des Beitrags liegt dabei auf der Frage nach der Anwendbarkeit etablierter völkerrechtlicher Verträge im Bereich des Cyberspace. Problematisiert wird außerdem die Zurechnung der Handlungen privater Akteure zu Staaten. Ferner wird die EU-Datenschutzgrundverordnung als Beispiel für eine konkrete Ausformung der staatlichen Pflicht zum Schutz der Privatsphäre im Cyberspace vorgestellt. Abschließend werden Maßnahmen zur Verbesserung der tatsächlichen Durchsetzung des Rechts auf Privatsphäre im Cyberspace vorgeschlagen.

The paper presents the multi-level system of international Human Rights protection, using the right to privacy in cyberspace as an example. Beside norms of global human rights law, particularities of regional human rights law based on the ECHR as well as European Union law are addressed. One of the main focuses of this paper is the question of the applicability of established international treaties in the field of cyberspace. In addition, the attribution of the actions of private actors to states is problematized. Furthermore, the EU General Data Protection Regulation is introduced as an example of a concrete implementation of the state's obligation to protect privacy in cyberspace. Finally, measures are proposed to improve the actual enforcement of the right to privacy in cyberspace.

[*] Der Verfasser studiert Rechtswissenschaft im siebten Fachsemester an der Ruprecht-Karls-Universität Heidelberg und ist wissenschaftliche Hilfskraft am Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht im Bereich von Prof. *Dr. Armin von Bogdandy, M.A.* Der Beitrag entstand als Seminararbeit im Sommersemester 2018 im Rahmen des Seminares „Völkerrecht im Cyberspace" bei Prof. *Dr. Anne Peters, LL.M. (Harvard).*

A. Einleitung

Nachdem *Edward Snowden* im Juni 2013 Dokumente über das weltweite Überwachungsprogramm des US-amerikanischen Geheimdienstes *NSA* veröffentlichte, hat die Sorge über den Zustand der Privatsphäre im Cyberspace neue Ausmaße angenommen. Die Dokumente haben gezeigt, dass die *NSA*, aber auch andere Geheimdienste, systematisch nahezu den gesamten Internetverkehr überwachen und detaillierte Profile einzelner Menschen angelegt haben. Heute, fünf Jahre später, ist immer noch unklar, inwieweit diese Praxis seitdem überarbeitet oder eingestellt wurde. Gleichzeitig hat der Cyberspace als Ort der privaten und öffentlichen Kommunikation weiter an Bedeutung gewonnen und bietet damit auch eine Vielzahl von Möglichkeiten, unkompliziert in die „digitale Privatsphäre" von Menschen einzudringen.

Dieser Beitrag setzt sich auseinander mit dem Recht auf Schutz der Privatsphäre im Cyberspace. Cyberspace im Sinne dieses Beitrags ist der globale Datenraum Internet, in dem Informationen zur Verfügung gestellt und übertragen werden. Dies umfasst unter anderem das Bereitstellen und Abrufen von Webseiten sowie die Nutzung digitaler Kommunikationsdienste wie Emails oder anderer Online-Messenger. Zunächst wird die Gewährleistung dieses Rechts im internationalen Menschenrechtsschutz analysiert, insbesondere mit dem Fokus auf Fragen der (extra-territorialen) Anwendbarkeit der einschlägigen Menschenrechtsinstrumente (**B.**). Darauffolgend wird das Recht auf Privatsphäre im europäischen Menschenrechtsschutz beleuchtet, auch im Hinblick auf die Datenschutzgrundverordnung der Europäischen Union, die derzeit für viel Aufsehen sorgt (**C.**).

B. Das Recht auf Privatsphäre im Cyberspace im internationalen Menschenrechtsschutz

Das Recht auf Schutz der Privatsphäre beschäftigt spätestens seit dem Ende des Zweiten Weltkriegs auch das Völkerrecht als Teil des internationalen Menschenrechtsschutzes.[1] Die Anwendung dieses Rechts im Cyberspace wirft besondere Fragen auf. „Der Cyberspace" stellt einen permanent globalen Raum dar, dessen Regulierung deshalb auch in ganz besonderen Maßen völkerrechtlicher Vereinbarungen bedarf.

I. Rechtsgrundlagen für das Recht auf Schutz der Privatsphäre

Das internationale Völkerrecht kennt (noch) keine expliziten, rechtsverbindlichen Verträge zum Recht auf Schutz der Privatsphäre im Cyberspace. Im Fol-

[1] *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, 2012, S. 59 ff.

genden werden daher zunächst die Rechtsgrundlagen für das allgemeine Recht auf Schutz der Privatsphäre vorgestellt, bevor im Weiteren das einschlägige, rechtlich nicht verbindliche *soft law*, wie bspw. Resolutionen der Generalversammlung der Vereinten Nationen (UN) und des UN-Menschenrechtsrates, dargestellt und auf die Besonderheiten der Anwendung und des Umfangs des Rechts auf Schutz der Privatsphäre im Cyberspace eingegangen wird.

1. Art. 12 der Allgemeinen Erklärung der Menschenrechte

Bereits in Art. 12 der am 10.12.1948 von der UN-Generalversammlung verabschiedeten Allgemeinen Erklärung der Menschenrechte (AEMR) heißt es, dass „[n]iemand willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden" darf. Art. 12 Abs. 2 AEMR manifestiert, dass jeder Mensch Anspruch auf Rechtsschutz gegen solche Eingriffe und Beeinträchtigungen hat. Die AEMR selbst ist kein rechtlich bindendes Dokument, die in ihr kodifizierten Rechte stellen jedoch teilweise schon zuvor existierendes oder nachträglich entstandenes Völkergewohnheitsrecht dar, welches als solches bindend ist.[2] Das in Art. 12 AEMR kodifizierte Recht umfasst neben dem Schutz des Privaten bzw. der Privatsphäre (Privatleben, Familie, Wohnung und Schriftverkehr) auch den Schutz der Persönlichkeit (Ehre und Ruf). Es ist ferner nicht nur ein reines Abwehrrecht, also ein Recht gegen staatliche Eingriffe, sondern gewährt auch explizit einen individuellen Anspruch auf rechtlichen Schutz gegen willkürliche Eingriffe (in das Privatleben) oder Beeinträchtigungen (der Persönlichkeit), die nicht zwingend staatlicher Natur sein müssen.[3] Die allgemeine Formulierung eines Anspruchs auf Rechtsschutz macht bereits in dieser ersten Kodifizierung des Rechts auf Schutz der Privatsphäre deutlich, dass es sich hierbei nicht nur um ein Recht handelt, welches das Verhältnis der Menschen zum Staat betrifft, sondern welches dem Staat Pflichten zur Durchsetzung des Rechts auch im Verhältnis von Privaten untereinander auferlegt.[4]

2. Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte

Hieran knüpft auch der nahezu wortgleiche Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte (IPbpR) an. Dieser wurde am 16.12.

[2] Gesonderte Stellungnahme Vize-Präsident *Ammoun*, in: *IGH*, Gutachten v. 21.6.1971, *Namibia*, ICJ-Reports 1971, 67 (76); *IGH*, *United States of America* v. *Iran*, Urt. v. 24.5. 1980, ICJ-Reports 1980, 3 (Rn. 91); *Herdegen*, Völkerrecht, 17. Aufl. 2018, § 47 Rn. 3.
[3] *Fassbender*, Menschenrechteerklärung, 2009, S. 107; *Ziemele*, Privacy, Right to, International Protection, MPEPIL, März 2009, Rn. 2.
[4] *Ziemele* (Fn. 3), Rn. 2.

1966 von der UN-Generalversammlung verabschiedet und trat am 23.3.1976, nachdem ihn 35 Staaten ratifiziert hatten, gemäß Art. 49 Abs. 1 IPbpR in Kraft. Als völkerrechtlicher Vertrag ist er für die derzeit 172 Vertragsstaaten[5] bindend.

Art. 17 IPbpR verbietet rechtswidrige und willkürliche Eingriffe in das Privatleben sowie den Schriftverkehr. Die ebenfalls geschützte Familie und Wohnung sind für das Recht auf Schutz der Privatsphäre im Cyberspace nicht von besonderer Bedeutung. Die Diskussion um Hasskommentare im Netz und ihrer Bekämpfung betrifft zwar auch den Anwendungsbereich des Schutzes der Ehre und des Rufs nach Art. 17 IPbpR, würde aber – insbesondere aufgrund ihrer Bezüge zur Meinungsfreiheit nach Art. 19 und dem Verbot der Hassrede nach Art. 20 IPbpR –[6] den Rahmen dieses Beitrags sprengen. Das Recht auf Privatsphäre im Sinne dieses Beitrags bezieht sich deshalb nur auf den Schutz des Privatlebens inklusive der persönlichen Kommunikation, nicht aber auf den Persönlichkeitsschutz im Sinne des Schutzes der Ehre und des Rufs.

Gemäß der Interpretation des UN-Menschenrechtsausschusses sollen staatliche Behörden ausschließlich Zugriff auf solche privaten Informationen erhalten, an deren Bekanntheit für die Behörden ein essenzielles gesellschaftliches Interesse besteht.[7] Der Schutz des Privatlebens umfasst auch den Datenschutz. So dürfen persönliche Informationen nicht ohne gesetzliche Grundlage gesammelt oder verarbeitet werden.[8] In Bezug auf die Sammlung durch staatliche Stellen zeigt sich hier die menschenrechtliche Dimension als Abwehrrecht, die Notwendigkeit einer gesetzlichen Grundlage für die Sammlung durch Private ist dagegen Ausfluss der staatlichen Schutzpflicht.[9] Zudem steht jeder Person ein Auskunftsanspruch gegenüber dem Verantwortlichen zu, ob und welche personenbezogenen Daten von ihr gesammelt wurden.[10] Der Schutz des „Schriftverkehrs" (engl. *correspondence*) umfasst nicht nur das geschriebene Wort, sondern den Schutz der Vertraulichkeit und Integrität jeglicher Form der Kommunikation, die grundsätzlich keinen Überwachungsmaßnahmen ausgesetzt sein darf.[11]

---

[5] *OHCHR*, Status of Ratification, Stand: 1.12.2018, abrufbar unter: http://indicators.ohchr.org (zuletzt abgerufen am 17.12.2018).

[6] Siehe zur Bedeutung sowie dem Zusammenspiel von Art. 19 und Art. 20 IPbpR im Kontext von Hassrede im Internet *Gagliardone/Gal/Alves/Martinez,* Countering Online Hate Speech, 2015, S. 19 ff.; zur Debatte im Rahmen der EMRK *Weber*, Manual on Hate Speech, 2009.

[7] *UN-Menschenrechtsausschuss*, CCPR General Comment No. 16, 8.4.1988, Rn. 7; *Schiedermair* (Fn. 1), S. 90.

[8] *UN-Menschenrechtsausschuss* (Fn. 7), Rn. 10.

[9] *Ebd.*

[10] *Ebd.*

[11] *Ebd.*, Rn. 8.

Art. 17 IPbpR schützt sowohl vor staatlichen, als auch vor Eingriffen natürlicher oder juristischer Personen.[12] Dem Staat wird durch Art. 17 Abs. 2 IPbpR die Pflicht aufgegeben, wirksamen Rechtsschutz gegen Eingriffe in das Recht auf Privatleben einzurichten.[13] Dies gilt gleichermaßen für Eingriffe staatlicher wie auch privater Akteure.[14] Er hat u. a. dafür Sorge zu tragen (wenn auch mit weitem Spielraum), dass private Telekommunikationsunternehmen ausreichende Sicherheitsstandards einhalten, um die Vertraulichkeit der Kommunikation zu gewährleisten.[15] Es zeigt sich somit, dass das Recht auf Privatsphäre nicht nur negativ – als Abwehrrecht – Schutz vor staatlichen Eingriffen bietet, sondern aufgrund des Rechts auf „*protection of the law*" vor Eingriffen eine positive Schutzpflicht des Staates im Bereich des horizontalen Verhältnisses Privater untereinander begründet wird.

3. *Soft Law* bezüglich des Rechts auf Schutz der Privatsphäre im Cyberspace

In den letzten Jahren haben die UN-Generalversammlung, der UN-Menschenrechtsrat und der vom Menschenrechtsrat eingesetzte Sonderberichterstatter zum Recht auf Privatsphäre[16] eine Vielzahl an Resolutionen und Berichten veröffentlicht, die als *soft law* die – in Teilen vertretene – Rechtsauffassung der Staatengemeinschaft darstellen und für die Entwicklung gewohnheitsrechtlicher Normen bzw. der Definition des Schutzbereiches des Rechts auf Privatsphäre relevant werden könnten. *Soft law* stellt, trotz seiner missverständlichen Bezeichnung, selbst kein bindendes Recht dar, kann aber als Initiator bei der Herausbildung bindender völkerrechtlicher Normen dienen oder als Rechtserkenntnisquelle bei der Auslegung völkerrechtlicher Verträge Bedeutung gewinnen.[17]

Bereits in der ersten Resolution zum Thema „*right to privacy in the digital age*", noch unter unmittelbarem Eindruck der Snowden-Veröffentlichungen zu den

[12] *UN-Generalversammlung*, Annotations on the Draft of International Covenants on Human Rights, 1.7.1955, A/2929, Chapter VI, Rn. 100 f.; *UN-Menschenrechtsausschuss* (Fn. 7), Rn. 1.
[13] *Nowak*, CCPR Commentary, 2. Aufl. 2005, Art. 17 Rn. 6 f.
[14] *Ebd.*
[15] *Schiedermair* (Fn. 1), S. 74 f.
[16] Der *Special Rapporteur on the Right to Privacy* wurde durch Beschluss des Menschenrechtsrats v. 26.3.2015 (A/HRC/RES/28/16) für einen Zeitraum von drei Jahren eingesetzt. Das Amt hat seit Juli 2015 der Malteser Prof. *Joseph Cannataci* inne. Am 22.3.2018 wurde das Mandat um drei weitere Jahre verlängert, A/HRC/RES/37/2. Weitere Informationen über die Arbeit des Sonderberichterstatters, insbesondere auch seine Jahresberichte, sind abrufbar unter: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx (zuletzt abgerufen am 17.12.2018).
[17] *v. Arnauld*, Völkerrecht, 3. Aufl. 2016, Rn. 277 f.; *Herdegen*, Völkerrecht, 17. Aufl. 2018, § 14 Rn. 5, § 20 Rn. 4.

Massenüberwachungsprogrammen der USA und anderer Staaten, zeigte sich die Generalversammlung „tief besorgt über die nachteiligen Auswirkungen, die das Überwachen […], einschließlich des extraterritorialen Überwachens […], auf die Ausübung und den Genuss der Menschenrechte haben können" und forderte die Staatengemeinschaft auf, das Recht auf Privatheit zu achten und zu schützen sowie Maßnahmen zu ergreifen, um den Verletzungen dieser Rechte ein Ende zu setzen.[18] Diese Aufforderung wurde auch in einer weiteren Resolution nochmals bekräftigt.[19] Auch der Menschenrechtsrat der Vereinten Nationen behandelte das Thema in mehreren Resolutionen[20] und beschloss im März 2015 schließlich die Ernennung eines Sonderberichterstatters für das Recht auf Privatheit, der dem Menschenrechtsrat und der Generalversammlung einen jährlichen Bericht vorlegen soll[21] und inzwischen auch eine Vielzahl nationaler Gesetzgebungsverfahren mit Bezug zum Recht auf Privatsphäre kommentiert hat.[22] Von besonderer Bedeutung ist außerdem noch der von Generalversammlung in seiner ersten Resolution zu diesem Thema angeforderte Bericht der Hohen Kommissarin der UN für Menschenrechte.[23] Die Berichte und die Resolutionen werden an dieser Stelle nicht einzeln ausführlich dargestellt, weil sie – wie oben bereits dargestellt – als *soft law* selbst nicht rechtlich verbindlich sind. Da sie aber Anhaltspunkte für die Interpretation rechtlich verbindlicher Völkerrechtsnormen, wie Art. 17 IPbpR, bieten, wird auf sie im Folgenden immer wieder verwiesen werden.

II. Besonderheiten im Cyberspace

Bei der Anwendung des Rechts auf Privatsphäre im Cyberspace gibt es einige Besonderheiten. Diese betreffen (**1.**) Abgrenzungsfragen, ab wann bereits – insbesondere bei der Auswertung von Metadaten – ein Eingriff in das Recht vorliegt, (**2.**) inwieweit aufgrund der globalen Gestalt des Cyberspace die einschlägigen Normen der Menschenrechtsverträge auch extraterritorial gelten und (**3.**) ob bei der Anwendbarkeit eine Unterscheidung zwischen Staatsbürgerinnen

[18] *UN-Generalversammlung*, The right to privacy in the digital age, 18.12.2013, A/RES/68/167.
[19] *UN-Generalversammlung*, The right to privacy in the digital age 18.12.2014, A/RES/69/166.
[20] *UN-Menschenrechtsrat*, The promotion, protection and enjoyment of human rights on the Internet, 26.6.2014, A/HRC/RES/26/13, sowie *UN-Menschenrechtsrat*, The right to privacy in the digital age, 26.3.2015, A/HRC/RES/28/16.
[21] Siehe hierzu Fn. 16.
[22] Siehe hierzu die Veröffentlichungen auf der Webseite des Sonderberichterstatters, abrufbar unter: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/CommentsLegislationPolicy.aspx (zuletzt abgerufen am 17.12.2018).
[23] *OHCHR*, The right to privacy in the digital age, 30.6.2014, A/HRC/27/37.

und Staatsbürgern auf der einen Seite und Ausländerinnen und Ausländern auf der anderen Seite zulässig ist.

1. Eingriffe

Art. 17 IPbpR schützt die Vertraulichkeit und Integrität jeglicher Form der Kommunikation und verbietet anlasslose Überwachung. Korrespondenz soll den Empfänger oder die Empfängerin erreichen, ohne dass sie in der Zwischenzeit geöffnet oder gelesen wurde.[24] Dies umfasst – auch wenn ihre Bedeutung in diesem Maße mit Sicherheit nicht von den Vertragsparteien vorhergesehen wurden – jedenfalls auch den Inhalt elektronischer Kommunikation.[25] Zu einer anderen Bewertung könnte man bei der Sammlung und Auswertung von Metadaten wie des Kontaktdatums des Empfängers, des Zeitpunkts der Kontaktaufnahme, des Aufenthaltsorts (bzw. der IP-Adresse) des Versenders und ähnlichem, kommen, also solchen Daten, die keine unmittelbaren Informationen über den Inhalt der Kommunikation offenbaren.[26] Regelmäßig werden sie auch bei grundsätzlich verschlüsselter Kommunikation, da sich die Verschlüsselung hierbei auf den Inhalt bezieht, unverschlüsselt übertragen.[27] Durch die Sammlung einer größeren Menge an Metadaten lassen sich exakte Persönlichkeitsprofile anlegen, die Informationen über den persönlichen Lebensstil, Krankheiten oder den Umgang mit Drogen enthalten.[28] Der Schutz des Privatlebens nach Art. 17 IPbpR umfasst deshalb auch den Schutz vor der massenhaften Sammlung und Auswertung von Metadaten.[29] Gleiches gilt für die Überwachung des Surfverhaltens einer Person. Es handelt sich hierbei zwar nicht um Kommunikation zwischen Menschen, sondern nur um das Abrufen von Informationen. Durch die Analyse großer Datensätze (*Big Data Analysis*) von Informationen, die einzeln betrachtet noch vergleichsweise unproblematisch, vielleicht sogar unpersönlich, sind, können jedoch exakte Persönlichkeits-

[24] *UN-Menschenrechtsausschuss* (Fn. 7), Rn. 8
[25] *Nowak* (Fn. 13), Art. 17 Rn. 47.
[26] *Meister*, Was sind eigentlich Metadaten?, Heinrich-Böll-Stiftung, 22.7.2014, abrufbar unter: https://www.boell.de/de/2014/07/22/was-sind-eigentlich-metadaten (zuletzt abgerufen am 17.12.2018).
[27] *Ebd.*
[28] *Adler*, What Metadata Reveals About You, The Century Foundation, 21.7.2016, abrufbar unter: https://tcf.org/content/facts/what-metadata-reveals-about-you/ (zuletzt abgerufen am 17.12.2018).
[29] *OHCHR* (Fn. 23), Rn. 19 f.; zustimmend *Peters*, Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extraterritorial Surveillance, in: Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair, 2017, S. 145 (149 f.).

profile erstellt werden.[30] Deshalb handelt es sich auch bei der Überwachung des Internetverkehrs, der nicht der inter-personalen Kommunikation zuzuordnen ist, um Eingriffe in das Privatleben einer Person.

2. Extraterritoriale Anwendung des Rechts auf Schutz der Privatsphäre im Cyberspace

Gemäß Art. 2 Abs. 1 IPbpR sind die Vertragsstaaten verpflichtet, die im Pakt anerkannten Rechte zu achten und sie allen in ihrem Gebiet (engl. *territory*) befindlichen und ihrer Herrschaftsgewalt (engl. *jurisdiction*) unterstehenden Personen zu gewährleisten. Das Zusammenspiel und die Interpretation der beiden Bedingungen ist umstritten. Insbesondere bei der Anwendung im Cyberspace zeigen sich außerordentliche Probleme. Der Wortlaut des Art. 2 Abs. 1 IPbpR stellt auf den Aufenthaltsort der betroffenen Person ab. Es ist also nicht die Frage von Bedeutung, ob durch eine Maßnahme selbst Hoheitsgewalt ausgeübt wird, sondern ob die von der Maßnahme betroffene Person der Hoheitsgewalt des agierenden Staates untersteht.[31] Bei Überwachungsmaßnahmen im Cyberspace fallen der Aufenthaltsort des Individuums und der Ort der staatlichen Maßnahme aber regelmäßig auseinander. So griff bspw. die NSA zum einen (in Kooperation mit dem BND) auf Internetknotenpunkte in Deutschland,[32] zum anderen jedoch auch auf unter anderem in den USA gelegenen Servern von *Google*, *Microsoft* und anderen Unternehmen zu.[33] Von beiden Maßnahmen waren aber auch deutsche Staatsbürger, die sich nicht auf US-amerikanischem Territorium aufhielten, betroffen. Ob und ggf. inwieweit die Verpflichtung zur Beachtung und Gewährleistung des Rechts auf Privatsphäre trotzdem greift, ist umstritten. Es haben sich im Wesentlichen vier verschiedene Ansätze herausgebildet:

---

[30] *Fenwick*, Psychographics: How big data is watching you, Hult International Business School, 2.2018, abrufbar unter: http://www.hult.edu/blog/psychographics-big-data-watching/ (zuletzt abgerufen am 17.12.2018).

[31] *Talmon*, Der Begriff der "Hoheitsgewalt" in Zeiten der Überwachung des Internet- und Telekommunikationsverkehrs durch ausländische Nachrichtendienste, JZ 2014, 783 (785).

[32] *Beuth*, BND und NSA: Ein neues Teil im Überwachungspuzzle, ZEIT Online, 26.6.2014, abrufbar unter: https://www.zeit.de/digital/datenschutz/2014-06/bnd-datenweiterleitung-nsa-seit-2004 (zuletzt abgerufen am 17.12.2018).

[33] *Ackermann*, Surveillance: US tech giants knew of NSA data collection, agency's top lawyer insists, The Guardian, 19.3.2014, abrufbar unter: https://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de (zuletzt abgerufen am 17.12.2018).

a) Streng territorialer Ansatz

Vor allem die USA vertreten, dass ein kumulatives Vorliegen beider Bedingungen notwendig sei, um den Geltungsbereich des IPbpR zu eröffnen. Ein Staat sei demnach nur zur Gewährleistung der Rechte des Paktes für diejenigen Personen verpflichtet, die sich innerhalb seines Staatsgebietes *und* unter seiner Herrschaftsgewalt befinden. Die US-amerikanische Regierung begründet diese Ansicht mit der Entstehungsgeschichte des IPbpR, bei der die amerikanische Vertreterin *Eleanor Roosevelt* deutlich machte, dass es nicht möglich sei, die Rechte des Paktes in komplexen Situation wie dem besetzten Deutschland zu garantieren.[34] Dieser Argumentation folgend lehnt die US-amerikanische Regierung bis heute die Anwendbarkeit der im IPbpR garantierten Rechte auf extraterritoriale Gefangenenlager oder Besatzungen fremden Territoriums ab.[35] Wendet man das Konzept auf Überwachungsmaßnahmen im Cyberspace an, gilt auch hier, dass der Schutz auf die Personen begrenzt, die sich in den USA aufhalten.[36] Für Menschen mit Aufenthaltsort außerhalb des US-amerikanischen Territoriums greift der Schutz dagegen nicht.

b) Extraterritoriale Anwendung bei der Ausübung von Herrschaftsgewalt

Diese Ansicht weisen u. a. der *IGH* und der UN-Menschenrechtsausschuss zurück. Hoheitsgewalt könne auch außerhalb des eigenen Staatsgebietes ausgeübt werden.[37] Art. 5 IPbpR verbiete es, Bestimmungen des Paktes auf eine Art und Weise auszulegen, in der sie dem Sinn und Zweck der im Pakt garantierten Rechte zuwiderlaufen.[38] Eine Auslegung von Art. 2 IPbpR, die Handlungen des Staates auf fremden Territorium erlaubt, welche ihm auf seinem eigenen Territorium verboten wären, sei deshalb unzulässig.[39] Die historische Auslegung von Art. 2 IPbpR unter Beachtung der *travaux préparatoires* mache deutlich, dass die konkrete Formulierung keinesfalls dafür gedacht war, Staaten von ihrer Verpflichtung zur Beachtung der Menschenrechte auf fremden Territorium zu ent-

[34] *UN-Wirtschafts- und Sozialrat*, Draft international covenant on human rights, 6.4.1950, E/CN.4/SR.138, Rn. 33 ff.
[35] *US-Bundesregierung*, Reply of the Government of the United States of America to the Report of the Five UNHCR Special Rapporteurs on Detainees in Guantánamo Bay, Cuba, 10.3.2006, International Legal Materials 2006, S. 742 (752 f.).
[36] So auch *Daskal*, Extraterritorial Surveillance Under the ICCPR … The Treaty Allows It!, Just Security, 7.3.2014, abrufbar unter: https://www.justsecurity.org/7966/extra territorial-surveillance-iccpr-its-allowed (zuletzt abgerufen am 17.12.2018).
[37] *IGH*, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion v. 9.7.2004, ICJ-Reports 2004, 136 (Rn. 107 ff.).
[38] *UN-Menschenrechtsausschuss*, *Burgos*, Auffassung v. 29.7.1981, Nr. 52/1979, CCPR/C/OP/1, S. 88, Rn. 12.3.
[39] *Ebd.*

binden.[40] Das Ziel sei lediglich gewesen, dass sich Staatsbürgerinnen und Staatsbürger, die sich außerhalb ihres Heimatstaates aufhalten, nicht gegenüber ihrem Heimatstaat auf Rechte berufen können, zu deren Durchsetzung und Beachtung der Heimatstaat verpflichtet sei.[41] Dies führe dazu, dass „Gebiet" und „Herrschaftsgewalt" alternative Bedingungen seien.[42] Wann immer ein Mensch sich innerhalb des Staatsgebietes einer Vertragspartei des Paktes aufhält, sei der Staat demnach zur Achtung der im Pakt verbürgten Rechte verpflichtet. Aber auch außerhalb seines Territoriums greife diese Verpflichtung, sofern die Menschen dort seiner Herrschaftsgewalt unterstehen. Dies sei bspw. bei einer Besatzung oder unmittelbarer physischer Gewalt der Fall.[43]

Die Anwendung dieser Ansicht im Cyberspace führt in der Literatur zu unterschiedlichen Ergebnissen:

aa) Keine Anwendung von Herrschaftsgewalt im Cyberspace

In Bezug auf den Cyberspace vertreten u. a. *Paust* und *Talmon*, dass eine Besatzung oder die Anwendung unmittelbarer physischer Gewalt die einzigen Ausnahmen vom Prinzip der Territorialität seien. Sofern sich ein von Überwachung betroffenes Individuum nicht im Territorium des handelnden Staates aufhalte und keine der beiden Ausnahmen greife, unterliege es auch nicht der Hoheitsgewalt des Staates. Auch in einer digitalisierten zunehmend auch virtuellen Welt führe das reine Abhören von Personen zu keiner Beschränkung ihrer Handlungsmöglichkeiten und könne dementsprechend auch keine Form der (virtuellen) Kontrolle darstellen.[44] Dies führe dazu, dass die Rechte aus dem IPbpR nicht anwendbar seien.[45]

bb) Virtuelle Kontrolle im Cyberspace

Peters hält dem entgegen, es komme nicht auf den Ort der Menschenrechtsverletzung an, sondern darauf, ob eine Beziehung zwischen dem Individuum und dem Staat besteht.[46] Sie rekurriert dabei auf die Auffassung des UN-Menschen-

[40] *IGH*, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion v. 9.7.2004, ICJ-Reports 2004, 136 (Rn. 109).
[41] *Ebd.*
[42] So auch *Peters* (Fn. 29), S. 152.
[43] *IGH*, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion v. 9.7.2004, ICJ-Reports 2004, 136 (Rn. 111); *UN-Menschenrechtsausschuss*, *Burgos*, Auffassung v. 29.7.1981, Nr. 52/1979, CCPR/C/OP/1, S. 88, Rn. 12.3.
[44] *Paust*, Can You Hear Me Now?: Private Communication, National Security, and the Human Rights Disconnect, Chicago Jounal of International Law 2015, 612 (625).
[45] *Talmon* (Fn. 31), S. 784 ff.
[46] *Peters* (Fn. 29), S. 152.

rechtsausschusses in *Burgos*, in dem es um die Entführung eines uruguayischen Staatsbürger in Buenos Aires, Argentinien durch den uruguayischen Geheimdienst ging.[47] Hier hat der Menschenrechtsausschuss festgehalten, dass eine Handlung, die auf eigenem Territorium aufgrund der Bestimmung des IPbpR unzulässig sei, auf fremden Territorium nicht erlaubt sein könne.[48] Entscheidend sei also nach *Peters*, ob eine tatsächliche, kausale Verknüpfung (engl. *factual causal link*) zwischen dem Staat und der Menschenrechtsverletzung bestehe, um seine Verantwortung für den Schutz der im Pakt gewährleisteten Rechte auszulösen.[49] Unmittelbare Überwachungsmaßnahmen, abhängig vom Ausmaß und der Intensität der Überwachung, stellten deshalb zwar keine Form der physischen Kontrolle dar, mündeten jedoch in eine virtuelle Kontrolle (engl. *virtual control*) , die einer Ausübung von Herrschaftsgewalt entspreche.[50]

c) Unterscheidung zwischen positiven und negativen Pflichten

Ein anderer Ansatz möchte auf die Unterscheidung zwischen positiven und negativen Pflichten des Staates abstellen. Die positive Pflicht des Staates, Menschenrechtsverletzungen von Dritten zu verhindern (Schutzpflicht), ist nur dann gegeben, wenn das entsprechende Gebiet einer effektiven Kontrolle unterliegt.[51] Negative Verpflichtungen zur Achtung von Menschenrechten, also die Verpflichtung des Staates, nicht ungerechtfertigt in Rechte von Individuen einzugreifen, griffen dagegen ohne territoriale Limitierung, da Staaten stets und überall in der Lage seien, Menschenrechtsverletzungen ihrer eigenen Organe und Vertretungen zu verhindern.[52] Auch hierbei falle deshalb jede Form der globalen Massenüberwachung unter den Anwendungsbereich des Paktes und bedürfe einer Rechtfertigung.[53]

---

[47] *UN-Menschenrechtsausschuss*, *Burgos*, Auffassung v. 29.7.1981, Nr. 52/1979, CCPR/C/OP/1, S. 88, Rn. 2.1-2.8.
[48] *Ebd.*, S. 88, Rn. 12.3.
[49] *Peters* (Fn. 29), S. 152 f.
[50] *Ebd.*, S. 156; *Peters*, Surveillance without Borders: The Unlawfulness of the NSA Panopticon, Part II, EJIL: Talk!, 4.11.2013, abrufbar unter: https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/ (zuletzt abgerufen am 17.12.2018). Dabei beruft sie sich auch auf die *OHCHR* (Fn. 23), Rn. 33, 34.
[51] *Milanovic*, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, Harvard International Law Journal 2015, 81 (118 f.).
[52] *Ebd.*, S. 119.
[53] *Milanovic*, Foreign Surveillance and Human Rights, Part 4: Do Human Rights Treaties Apply to Extraterritorial Interferences with Privacy?, EJIL: Talk!, 29.11.2013, abrufbar unter: https://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-4-do-human-rights-treaties-apply-to-extraterritorial-interferences-with-privacy (zuletzt abgerufen am 17.12.2018).

d) Eigene Stellungnahme

Das Konzept, welches die Möglichkeit der Anwendung von Herrschaftsgewalt im Cyberspace grundsätzlich verneint, verkennt meines Erachtens die heutige Bedeutung des Cyberspace. Tatsächliche Kontrolle über eine Person liege demnach nur bei der Möglichkeit des physischen Zugriffs auf die Person vor.[54] Tatsächlich ist es jedoch bei bestimmten Menschenrechten, wie bspw. dem Recht auf Eigentum oder strafrechtlichen Verfahrensregeln, völlig anerkannt, dass der Staat auch ohne direkte Einwirkungsmöglichkeiten auf die Person Herrschaftsgewalt ausüben kann. Dies ist bspw. der Fall, wenn das Eigentum einer sich im Ausland befindlichen Person konfisziert wird[55] oder wenn Strafverfahren in Abwesenheit des Angeklagten durchgeführt werden.[56] Es kommt also nicht darauf, ob physisch auf eine Person zugegriffen werden kann, sondern ob es dem Staat möglich ist, in ihre absolut geschützten Rechtspositionen einzugreifen – unabhängig von ihrem tatsächlichen Aufenthaltsort. Wer die Daten einer Person kontrolliert, hat Macht über sie. Spätestens wenn diese Daten genutzt werden – sei es zur zielgerichteten Werbung (engl. *targeted advertising*) im Privatsektor, zur Manipulation von Wahlen[57] oder zur Kontrolle von Volksgruppen[58] – zeigt sich, dass aufgrund gesammelter Daten massiv auf Personen eingewirkt werden kann, sie also der Herrschaftsgewalt des Datenbesitzenden unterstehen.

Überzeugend sind deshalb die Ansätze der *virtual control* sowie der Unterscheidung zwischen positiven und negativen Pflichten des Staates, die regelmäßig wohl zum gleichen Ergebnis führen. Als Indiz für die effektive Kontrolle eines Staates über eine Person kann die kausale Verknüpfung zwischen dem Eingriff und einer Handlung dieses Staates dienen. Ist es einem Staat möglich, in einer

---

[54] So im Ergebnis *Talmon* (Fn. 31), S. 784 f.

[55] *Nyst*, Interference-Based Jurisdiction Over Violations of the Right to Privacy, EJIL: Talk!, 21.11.2013, abrufbar unter: https://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-to-privacy/ (zuletzt abgerufen am 17.12.2018). Unter anderem bezieht sie sich hierbei auch auf *EGMR*, *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Şirketi* v. *Irland*, Urt. v. 30.6.2005, Rs. 45036/98, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-69564 (zuletzt abgerufen am 17.12.2018).

[56] Ständige Rechtsprechung des *EGMR*, u. a. in *Colozza* v. *Italien*, Urt. v. 12.2.1985, Rs. 9024/80, Rn. 27 ff., abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-57462 (zuletzt abgerufen am 17.12.2018); *Poitrimol* v. *Frankreich*, Urt. v. 23.11.1993, Rs. 14032/88, Rn. 35, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-57858 (zuletzt abgerufen am 17.12.2018).

[57] *Beuth*, US-Wahl: Facebooks versteckter Fingerzeig auf Russland, ZEIT Online, 28.4.2017, abrufbar unter: https://www.zeit.de/digital/internet/2017-04/us-wahl-facebook-russland-manipulation (zuletzt abgerufen am 17.12.2018).

[58] *Lee*, China: Die AAA-Bürger, ZEIT Online, 30.11.2017, abrufbar unter: https://www.zeit.de/digital/datenschutz/2017-11/china-social-credit-system-buergerbewertung (zuletzt abgerufen am 17.12.2018).

gewissen Intensität auf die Rechtsgüter einer Person einzuwirken, befindet sich diese unter seiner Herrschaftsgewalt. Der Aufenthaltsort in einem bestimmen Staatsgebiet kann in einer Welt, in der räumliche Distanzen zunehmend irrelevant werden, lediglich als Indiz für das Vorliegen von Herrschaftsgewalt dienen, nicht jedoch notwendiges Kriterium sein. Gleichzeitig dürfte solch eine Einwirkung auch stets ein Handeln des Staates darstellen, er sich also in seinem negativen Pflichtenbereich bewegen, sodass der Anwendungsbereich auch nach der zweiten der beiden Ansichten eröffnet ist.

3. Personeller Anwendungsbereich des Rechts auf Schutz der Privatsphäre

Neben der Frage der Territorialität wird auch die Frage des personellen Anwendungsbereichs des Rechts auf Schutz der Privatsphäre im Cyberspace diskutiert.

So vertreten die USA den Ansatz, dass US-Staatsbürger und Einwohner der USA einem besonderen Schutz unterlägen, der jedoch nicht für Ausländer bzw. nicht in den USA sesshafte Personen gelte.[59] Grundsätzlich ist eine Differenzierung nach Staatsbürgerschaft bei Grundrechten, die durch nationale Verfassungen garantiert werden, durchaus üblich.[60] Anders sieht es dagegen bei den durch internationale Verträge garantierten Menschenrechten aus. So gebietet Art. 2 Abs. 1 IPbpR, dass die im Pakt verbürgten Rechte unabhängig von „Rasse, Hautfarbe, […] nationaler Herkunft, […] oder des sonstigen Status" einer Person gewährleistet werden müssen. Eine Unterscheidung auf Basis der Nationalität bzw. der Staatsbürgerschaft ist damit nur bei politischen Rechten nach Art. 25 IPbpR zulässig.[61] Sachliche Gründe für eine Differenzierung beim Recht auf Privatsphäre sind aber nicht erkennbar, da es sich hierbei nicht um spezifisch politische Rechte handelt.[62] Der UN-Menschenrechtsausschuss hat insbesondere beim Recht auf Privatsphäre im Cyberspace deutlich gemacht, dass dieses unabhängig vom Aufenthaltsort oder der Nationalität von Individuen gewährleistet werden muss.[63] Die Unterscheidung zwischen In- und Ausländern bei der Überwachungstätigkeit von Geheimdiensten ist mithin nicht mit dem IPbpR vereinbar. Das Recht auf Privatsphäre gewährleistet somit unabhängig von der Staatsangehörigkeit der betroffenen Person, ihrem Aufenthalts-

[59] Diskussion bei *Milanovic* (Fn. 51), S. 87 ff.
[60] So kennt bspw. auch die deutsche Verfassung „Deutschen-Grundrechte" wie u. a. die Versammlungsfreiheit (Art. 8 GG), die Vereinigungsfreiheit (Art. 9 GG) und die Berufsfreiheit (Art. 12 GG). Fast ausnahmslos ist weltweit bspw. auch das Wahlrecht an die Staatsbürgerschaft einer Person geknüpft.
[61] *UN-Menschenrechtsausschuss*, CCPR General Comment No. 18, Rn. 7 f.
[62] So auch *Peters* (Fn. 29), S. 162 f.
[63] *UN-Menschenrechtsausschuss*, Concluding Observations on the Fourth Periodic Report of the United States of America, 23.4.2014, CCPR/C/USA/CO/4, Rn. 22.

ort oder dem Ort, an dem die Überwachungsmaßnahme durchgeführt wird, grundsätzlich Schutz vor staatlichen Eingriffen.

III. Schranken des Rechts auf Schutz der Privatsphäre

Das Recht auf Schutz der Privatsphäre wird jedoch nicht schrankenlos gewährleistet. Eingriffe in Art. 17 IPbpR können gerechtfertigt sein, sofern sie keine „willkürlichen oder rechtswidrigen" Eingriffe darstellen. Sie bedürfen einer Gesetzesgrundlage, die selbst mit den Zielen des Paktes vereinbar sein muss, und keinesfalls den Kern des Rechts beeinträchtigen darf.[64] Das Verbot des willkürlichen Eingriffs betrifft nicht nur prozessuale Fragen, sondern gebietet auch die Erforderlichkeit und Angemessenheit der durchgeführten Maßnahme.[65] Der UN-Menschenrechtsausschuss sowie die Hohe Kommissarin für Menschenrechte haben betont, dass auch für die Umsetzung des Rechts auf Privatsphäre im Cyberspace die Prinzipien der Legalität, Geeignetheit und Angemessenheit beachtet werden müssen.[66]

Eine anlassbezogene Einzelfallüberwachung könnte wohl – je nach konkretem Fall – regelmäßig diese Kriterien erfüllen. Eine anlasslose Massenüberwachung kann dies, wie im Folgenden gezeigt wird, nicht: So fehlte bspw. für das Überwachungsprogramm der NSA schon eine ausreichende Gesetzesgrundlage, sodass die Überwachung den Grundsatz der Legalität verletzte.[67] Ferner ist zweifelhaft, ob die Analyse solch enormer Datenmengen überhaupt möglich ist.[68] Die Datensammlung ist also auch nicht bzw. nur sehr begrenzt geeignet, das Ziel der Bekämpfung des globalen Terrorismus zu erfüllen. Zwar sieht bspw. *Peters* dies als Argument dafür, dass die massenhafte Speicherung von Daten nicht *per se* unverhältnismäßig sei, gerade weil Geheimdienste nicht in der Lage seien, jedes einzelne Datum zu überprüfen.[69] Dem ist jedoch nicht zu folgen. Sofern man das Argument konsequent weiterdenkt, könnte sogar eine totale Überwachung jedes Lebensbereichs verhältnismäßig sein, solange der Zugriff auf die Daten ausreichend reguliert wird. Überwachung zeichnet sich aber zunächst durch die Speicherung der Daten, nicht erst durch ihre Auswertung aus.

---

[64] *UN-Menschenrechtsausschuss* (Fn. 7), Rn. 3; *Peters* (Fn. 29), S. 157, sich auf *UN-Menschenrechtsausschuss*, General Comment No 27, Rn. 13 beziehend.
[65] *UN-Menschenrechtsausschuss*, *Canepa*, Auffassung v. 3.4.1997, Nr. 558/1993, CCPR/C/59/D/558/1993, Rn. 11.4; *Schiedermair* (Fn. 1), S. 78; in Bezug auf Eingriffe in das Recht auf Privatsphäre im Cyberspace *Peters* (Fn. 29), S. 157; *OHCHR* (Fn. 23), Rn. 23.
[66] *UN-Menschenrechtsausschuss* (Fn. 63), Rn. 22; *OHCHR* (Fn. 23), Rn. 23.
[67] *Peters* (Fn. 29), S. 158.
[68] *Maass*, Inside NSA, Officials Privately Criticize "Collect It All" Surveillance, The Intercept, 28.5.2015, abrufbar unter: https://theintercept.com/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance (zuletzt abgerufen am 17.12.2018).
[69] *Peters* (Fn. 29), S. 161.

Sie entfaltetet unmittelbar einen einschüchternden Effekt (engl. *chilling effect*), der Auswirkung auf die Handlungen und insbesondere die Meinungsfreiheit von Individuen hat.[70] Des Weiteren bringt eine umfangreiche Datensammlung auch in einer demokratischen Gesellschaft stets ein immenses Missbrauchsrisiko mit sich, weil immer die Gefahr des Zugriffs durch Unberechtigte oder eines gesellschaftlichen Wandels hin zu autoritären Strukturen besteht. Auch die derzeit technisch begrenzten Auswertungsmöglichkeiten werden sich zukünftig durch *Big Data* und die Nutzung künstlicher Intelligenz deutlich erweitern.[71]

Das anlasslose, massenhafte Sammeln von Daten, das einen Eingriff in das Recht auf Privatsphäre von Millionen, wenn nicht Milliarden von Individuen darstellt, kann deshalb nicht gerechtfertigt werden.

IV. Rechtsschutz bei Verletzungen des Rechts auf Schutz der Privatsphäre

Rechtsschutzmöglichkeiten bei Verletzungen des Rechts auf Schutz der Privatsphäre ergeben sich auf zwei Ebenen: So manifestiert Art. 17 Abs. 2 IPbpR den Anspruch auf effektiven Rechtsschutz auf nationaler Ebene. Inwieweit ein solcher Rechtsschutz tatsächlich gewährleistet ist, richtet sich nach der Umsetzung in den jeweiligen nationalen Rechtsordnungen. Grundsätzlich gilt hierbei, dass im Rahmen der Klagebefugnis die persönliche Betroffenheit von einem Überwachungsprogramm mangels entsprechender Möglichkeit des Nachweises nicht bewiesen werden muss.[72] Die bloße Existenz eines Überwachungsprogramms reicht – aufgrund des *chilling effects*, den es u. a. für die Meinungsfreiheit entwickelt – aus, um einen Eingriff in das Recht auf Privatsphäre zu manifestieren.[73]

Abgesehen von den nationalen Rechtsschutzmöglichkeiten haben 116 Staaten das Fakultativprotokoll zum IPbpR vom 16.12.1966 (Fakultativprotokoll) ratifiziert.[74] Art. 2 des Fakultativprotokolls ermöglicht es Individuen, Beschwerden über die Verletzung von Menschenrechten durch den jeweiligen Staat, nach

[70] Siehe bspw. zu den Auswirkungen der Veröffentlichung der Überwachung durch die NSA auf die Nutzung von *Wikipedia*: *Penney*, Chilling Effects: Online Surveillance and Wikipedia Use, Berkeley Tech. Law Journal 2016, 117 ff.
[71] Siehe hierzu bspw. *Ferguson*, The High-Definition, Artificially Intelligent, All-Seeing Future of Big Data Policing, American Civil Liberties Union, 4.4.2018, abrufbar unter: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/high-definition-artificially-intelligent-all (zuletzt abgerufen am 17.12.2018).
[72] So jedenfalls u. a. die ständige Rechtsprechung des *EGMR*, siehe dazu unten **C. I. 4**. Teilweise wird erfordert, dass wenigstens die Wahrscheinlichkeit, von einer Überwachung betroffen zu sein, hinreichend dargelegt wird, siehe hierzu bzgl. Deutschland *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 81 ff. (juris).
[73] *OHCHR* (Fn. 23), Rn. 20.
[74] *OHCHR* (Fn. 5).

Ausschöpfung aller innerstaatlichen Rechtsmittel, vor den Menschenrechtsausschuss zu bringen. Dieser veröffentlicht daraufhin eine Auffassung zu der jeweiligen Beschwerde, die zwar kein rechtlich bindendes Urteil darstellt, von den Vertragsstaaten jedoch nach den Grundsätzen von Treu und Glauben beachtet werden muss.[75] Somit bietet sich auch für von Überwachung betroffene Personen, nach Ausschöpfung des nationalen Rechtswegs, die Möglichkeit einer Mitteilung an den Menschenrechtsausschuss. Zu beachten ist jedoch, dass das Fakultativprotokoll nur für die Staaten gilt, die es ratifiziert haben. Trotz der insgesamt großen Verbreitung gehören hierzu u. a. nicht China, die USA und Großbritannien.[76]

V. Zurechnung der Handlungen privater Akteure

Die durch die *Snowden*-Enthüllungen bekanntgewordenen Überwachungsprogramme zeichnen sich dadurch aus, dass nicht nur unmittelbare staatliche Überwachung, bspw. durch technische Installationen zum Abhören von Internetkabeln, stattfindet, sondern auch umfangreich mit Privatfirmen kooperiert wird.[77] Diese Kooperation, wenn auch noch unklar ist, ob sie vonseiten der Unternehmen freiwillig oder aufgrund gesetzlicher Verpflichtungen erfolgte, ist ein essenzieller Baustein der *NSA*-Überwachung.[78]

Die Zurechnung der Handlungen privater Akteure zu einem Staat erfordert gemäß Art. 8 der Articles on State Responsibility (ASR), dass eine Person im Auftrag oder unter der Leitung und Kontrolle des Staates handelt. Die ASR wurden von der UN-Völkerrechtskommission entwickelt und später von der Generalversammlung in einer Resolution verabschiedet.[79] Sie sind selbst nicht rechtsverbindlich, stellen aber teilweise, wie Art. 8 ASR,[80] Völkergewohnheitsrecht dar.[81] Insofern Private im Auftrag eines Staates i. S. v. Art. 8 ASR handeln, agieren sie dabei nicht als *de facto*-Staatsorgane, sondern als Private. Ihre Handlungen rufen jedoch die Verantwortlichkeit des Staates bzw. der Organe, welche

[75] *Tomuschat*, Human Rights Committee, MPEPIL, Oktober 2010, Rn. 14.
[76] *OHCHR* (Fn. 5).
[77] *Ackermann* (Fn. 33).
[78] *Groll*, How American Companies Enable NSA Surveillance, Foreign Policy, 4.10.2016, abrufbar unter: http://foreignpolicy.com/2016/10/04/how-american-companies-enable-nsa-surveillance (zuletzt abgerufen am 17.12.2018).
[79] *UN Generalversammlung*, Verantwortlichkeit der Staaten für völkerrechtswidrige Handlungen, 12.12.2001, A/RES/56/83.
[80] *IGH*, *Genocide Convention* (Bosnia and Herzegovina v. Serbia and Montenegro), Urt. v. 26.2.2007, ICJ-Reports 2007, 43 (Rn. 398).
[81] *Kees*, Responsibility of States for Private Actors, MPEPIL, März 2011, Rn. 11 ff.

die Instruktionen geben, hervor.[82] Dies gilt jedoch nur, sofern der Staat hierbei tatsächliche Kontrolle (engl. *effective control*) über die Privaten ausübt oder zumindest klare Anweisungen bezüglich jeder einzelnen Handlung, die zu einer Menschenrechtsverletzung führt, gibt.[83]

Dies lässt sich bei den genannten Kooperationen zwischen Geheimdiensten und privaten Unternehmen wohl nicht annehmen. Diese dürften hierbei regelmäßig für eigene oder vertragliche Zwecke, bspw. für personalisierte Werbung, als E-Mail- oder Cloud-Provider, persönliche Daten der Nutzerinnen und Nutzer gesammelt und diese darauffolgend, teilweise aufgrund gerichtlicher Verfügungen, teilweise auf freiwilliger Basis, den Geheimdiensten zur Verfügung gestellt haben.[84] Da die Sammlung selbst aber nicht im Auftrag des Staates oder aufgrund der Kontrolle durch ihn stattfand, ist eine Zurechnung der Handlungen dieser privaten Akteure zum Staat nicht möglich. Sofern der Staat die Daten später jedoch anfordert und auswertet, handelt es sich hierbei um einen Eingriff – ggf. sogar eine Verletzung – des Rechts auf Schutz der Privatsphäre, die unmittelbar durch ihn erfolgt und keiner Zurechnung bedarf.

C. Recht auf Privatsphäre im Cyberspace im europäischen Menschenrechtsschutz

Nicht nur der internationale Menschenrechtsschutz, sondern auch regionale Instrumente des Menschenrechtsschutzes kennen das Recht auf Privatsphäre. Im nicht-europäischen regionalen Menschenrechtsschutz ist das Recht auf Privatsphäre u. a. in Art. 11 der Amerikanischen Menschenrechtskonvention (AMRK) anerkannt. In der Afrikanischen Charta der Menschenrechte und der Rechte der Völker wird dagegen bemerkenswerterweise – und in Abgrenzung zum IPbpR, der EMRK und der AMRK – lediglich die Familie, nicht jedoch die Privatsphäre des Einzelnen als schützenswert anerkannt.[85] Es überstiege aber den Rahmen dieses Beitrags, auch diese beide Menschenrechtsinstrumente zu behandeln. Im Folgenden wird deshalb ausschließlich das Recht auf Schutz der Privatsphäre im Cyberspace in der EMRK und dem Primärrecht der EU analysiert. Als Beispiel für die Umsetzung staatlicher Schutzpflichten wird zudem die Datenschutzgrundverordnung der EU dargestellt. Ebenfalls nicht eingegangen werden kann auf die Konvention 108 des Europarates; das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

[82] *IGH*, *Genocide Convention* (Bosnia and Herzegovina v. Serbia and Montenegro), Urt. v. 26.2.2007, ICJ-Reports 2007, 43 (Rn. 397).
[83] *Ebd.*, Rn. 400.
[84] *Groll* (Fn. 78).
[85] *Schiedermair* (Fn. 1), S. 114 f.

I. Art. 8 der Europäischen Menschenrechtskonvention

In Art. 8 der EMRK heißt es, dass jede Person „das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz" hat. Art. 8 EMRK stellt zunächst ein klassisches Abwehrrecht dar, das vor staatlicher Einflussnahme auf den privaten Lebensbereich schützen soll.[86] Dies zeigt auch Art. 8 Abs. 2 EMRK, der als Schrankenregelung die Möglichkeiten eines staatlichen Eingreifens in dieses Recht definiert. Ferner umfasst Art. 8 EMRK positive Pflichten, also Schutz- und Gewährleistungspflichten. Der Staat ist verpflichtet, auch im horizontalen Verhältnis zwischen Privaten einen ausreichenden Schutz vor Verletzungen des Rechts auf Privatsphäre zu bieten.[87]

1. Schutzbereich

Die EMRK unterscheidet, wie auch der IPbpR, zwischen dem Recht auf Achtung des Privatlebens und der Achtung der privaten Korrespondenz. Diese Unterscheidung kann in einigen Bereichen aber nicht trennscharf formuliert werden. Dem Begriff der Korrespondenz unterfallen nicht nur der Schriftverkehr, sondern auch moderne Kommunikationsformen wie Telefonie und E-Mails.[88] Dementsprechend stellt die Beschlagnahme elektronisch gespeicherter Daten einen Eingriff in das Recht auf Achtung der Korrespondenz dar.[89] Auch die Sammlung personenbezogener Daten stellt einen Eingriff in den Schutzbereich des Rechts auf Achtung des Privatlebens dar. Dies ist unabhängig davon der Fall, ob auf die gespeicherten Informationen später auch zugegriffen wird.[90] So stellt bspw. eine systematische GPS-Überwachung zum Zwecke der Erstellung eines Bewegungsprofils einen Eingriff in Art. 8 EMRK dar.[91] Auch die Speicherung von Metadaten, die im Rahmen elektronischer Kommunika-

[86] *Schiedermair* (Fn. 1), S. 170.
[87] *Meyer-Ladewig/Nettesheim*, in: Meyer-Ladewig/Nettesheim/v. Raumer, EMRK, 4. Aufl. 2017, Art. 8 Rn. 2, 5.
[88] *EGMR*, *Klass u.a.* v. *Deutschland*, Urt. v. 6.9.1978, Rs. 5029/71, Rn. 41, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-57510 (zuletzt abgerufen am 17.12.2018); *Schiedermair* (Fn. 1), S. 221.
[89] *EGMR*, *Wieser u. Bicos Beteiligungen GmbH* v. *Österreich*, Urt. v. 16.10.2007, Rs. 74336/01, Rn. 45, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-82711 (zuletzt abgerufen am 17.12.2018).
[90] *EGMR*, *Leander* v. *Schweden*, Urt. v. 26.3.1987, Rs. 9248/81, Rn. 48, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-57519 (zuletzt abgerufen am 17.12.2018); *EGMR*, *Amann* v. *Schweiz*, Urt. v. 16.2.2000, Rs. 27798/95, Rn. 69, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-58497 (zuletzt abgerufen am 17.12.2018).
[91] *EGMR*, *Big Brother Watch* v. *Vereinigtes Königreich*, Urt. v. 13.9.2018, Rs. 58170/13, 62322/14, 24960/15, Rn. 355 f., abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-186048 (zuletzt abgerufen am 17.12.2018).

tion oder des Surfens im Internet entstehen, ist ein Eingriff in Art. 8 EMRK.[92] Der *Europäische Gerichtshof für Menschenrechte* (*EGMR*) hat insbesondere deutlich gemacht, dass Metadaten keinesfalls *per se* weniger sensibel und deshalb weniger schützenswert als der Inhalt der Kommunikation sind.[93] Ein Eingriff liegt regelmäßig auch bei der Videoüberwachung öffentlicher Orte vor. Dies ist nur dann nicht der Fall, wenn die Aufnahmen nicht gespeichert werden. Bei der systematischen Speicherung solcher Aufnahmen, insbesondere wenn diese auch noch mit Gesichtserkennungssoftware verbunden wird,[94] handelt es sich dagegen um einen – je nach Ausmaß und Verarbeitung der Videoüberwachung – intensiven Eingriff in das Recht auf Privatsphäre.[95]

2. Territorialer und personeller Anwendungsbereich der EMRK

Gemäß Art. 1 EMRK verpflichten sich die Vertragsstaaten, allen unter ihrer Hoheitsgewalt stehenden Personen die Rechte und Freiheiten der EMRK zukommen zu lassen. Der *EGMR* hat sich in seiner Rechtsprechung umfassend mit der Frage des territorialen Anwendungsbereichs auseinandergesetzt. Außerhalb des Staatsgebietes kann eine Person dann der Hoheitsgewalt eines Staates unterliegen, wenn sie sich in einem vom Staat effektiv kontrollierten Gebiet aufhält.[96] Der *EGMR* hat 2001 in *Bankovic* – im Rahmen der Zulässigkeit einer Beschwerde bezüglich des Bombardements eines Radio- und Fernsehsenders während des Kosovo-Krieges – entschieden, dass dieses Kriterium nicht erfüllt sei, wenn lediglich die Ursache und Wirkung einer staatlichen Handlung eine Person treffen und diese sich nicht in einem ansonsten effektiv kontrolliertem Gebiet aufhält.[97] In späteren Entscheidungen scheint der *EGMR* diese Kriterien jedoch wieder etwas aufgeweicht zu haben und primär darauf abzustellen, inwiefern eine Menschenrechtsverletzung einem Staat eindeutig zurechenbar ist,

---

[92] *EGMR*, *Big Brother Watch* v. *Vereinigtes Königreich*, Urt. v. 13.9.2018, Rs. 58170/13, 62322/14, 24960/15, Rn. 355 f., abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-186048 (zuletzt abgerufen am 17.12.2018).

[93] *EGMR*, *Uzun* v. *Deutschland*, Urt. v. 2.9.2010, Rs. 35623/05, Rn. 51 f., abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-100293 (zuletzt abgerufen am 17.12.2018).

[94] Zum Pilotprojekt einer Videoüberwachung mit Gesichtserkennung in Deutschland siehe *Jens Wienung*, Gesichtserkennung am Südkreuz: Sicherheit - zu Lasten der Grundrechte, tagesschau.de, 15.12.2017, abrufbar unter: https://www.tagesschau.de/inland/gesichtserkennung-141.html (zuletzt abgerufen am 17.12.2018).

[95] *EGMR*, *Peck* v. *Vereinigtes Königreich*, Urt. v. 28.1.2003, Rs. 44647/98, Rn. 59, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-60898 (zuletzt abgerufen am 17.12.2018).

[96] *EGMR*, *Loizidou* v. *Türkei (Preliminary Objections)*, Urt. v. 23.3.1995, Rs. 15318/89, Rn. 62, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-58007 (zuletzt abgerufen am 17.12.2018).

[97] *EGMR*, *Bankovic et al.* v. *Belgien und 16 weitere Staaten*, Entscheidung über die Zulässigkeit v. 12.12.2001, Rs. 52207/99, Rn. 75, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-22099 (zuletzt abgerufen am 17.12.2018).

um als *jurisdictional link*, also eine die Jurisdiktion der EMRK begründende Verknüpfung, zu wirken.[98] Der *EGMR* hat zudem festgestellt, dass die EMRK zu einem europäischen *ordre public* gehört. Deshalb ist ein Konventionsstaat, auch wenn er auf dem Hoheitsgebiet eines anderen Konventionsstaates – innerhalb des europäischen *espace juridique* – handelt, bspw. im Falle einer Besatzung, zur Achtung der Rechte und Freiheiten der EMRK verpflichtet sei.[99]

Bei Achtung des Rechts auf Privatsphäre im Cyberspace sind die beiden letzten Konzepte, der *jurisdictional link* sowie der europäische *ordre public*, von besonderer Bedeutung. So ließe sich der Gedanke eines europäischen *ordre public*, einer europäischen öffentlichen Ordnung, der für den Zustand der Besatzung eines Territoriums einer anderen Vertragspartei entwickelt wurde, zu einer generellen Verpflichtung der Beachtung der EMRK für solche Handlungen weiterentwickeln, die Wirkung für Personen entfalten, welche der unmittelbaren Hoheitsgewalt eines anderen Konventionsstaates unterliegen.[100] So wäre jedenfalls der menschenrechtliche Schutz innerhalb aller Vertragsstaaten der EMRK, auch vor Überwachungsmaßnahmen anderer Mitgliedstaaten, sichergestellt.

Noch weiter ginge die Anwendung des Konzepts des *jurisdictional links* im Cyberspace. Sofern es nur auf die Verursachung bzw. Zurechnung einer Menschenrechtsverletzung zu einem Staat ankommt, damit eine Person dessen Hoheitsgewalt untersteht, könnte sich der *EGMR* einem weiten Konzept der Hoheitsgewalt im Cyberspace öffnen.[101] In der Folge wären die Konventionsstaaten verpflichtet, auch bei (internationalen) Überwachungsmaßnahmen, die

[98] Ausschließlich auf die Kausalität einer Handlung des Staates für das Vorliegen von Hoheitsgewalt abstellend *EGMR*, *Pad et al.* v. *Türkei*, Entscheidung über die Zulässigkeit v. 28.6.2007, Rs. 60167/00, Rn. 53 f., abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-81672 (zuletzt abgerufen am 17.12.2018); das Konzept des *jurisdictional links* wurde darauffolgend in *EGMR*, *Al-Skeini et al.* v. *Vereinigtes Königreich*, Urt. v. 7.7.2011, Rs. 55721/07, Rn. 150, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-105606 (zuletzt abgerufen am 17.12.2018) entwickelt.

[99] *EGMR*, *Zypern* v. *Türkei*, Urt. v. 10.5.2001, Rs. 25781/94, Rn. 78, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-59454 (zuletzt abgerufen am 17.12.2018).

[100] So *Schübel-Pfister*, in: Karpenstein/Mayer, EMRK, 2. Aufl. 2015, Art. 1 Rn. 32.

[101] Jedenfalls als eine Möglichkeit der Begründung für eine Konventionsbindung aufwerfend: *ebd.;* basierend auf *EGMR*, *Al-Skeini et al.* v. *Vereinigtes Königreich*, Urt. v. 7.7.2011, Rs. 55721/07, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-105606 (zuletzt abgerufen am 17.12.2018), wo der *EGMR* ausschließlich auf die Verursachung des Tods der beteiligten Personen abgestellt hat, um eine Bindung des Vereinigten Königreich an die EMRK zu bejahen (Rn. 150): „*It is not disputed that the deaths* […] *were* caused *by the acts of British soldiers* […]. It follows that in all these cases there was a jurisdictional link for the purposes of Article 1 of the Convention *between the United Kingdom and the deceased.*" [Hervorhebung durch den Verfasser].

nicht ihre Einwohnerinnen und Einwohner betreffen, die in der Konvention verbrieften Rechte zu gewährleisten.

Im personellen Anwendungsbereich ist wie auch beim IPbpR eine Differenzierung nach Herkunft oder Nationalität einer Person nicht zulässig. Das in Art. 14 EMRK kodifizierte Diskriminierungsverbot ist dabei nahezu wortgleich mit Art. 2 Abs. 1 IPbpR.

3. Schranken nach Art. 8 Abs. 2 EMRK

Die Schranken des Rechts auf Achtung des Privatlebens definiert Art. 8 Abs. 2 EMRK. Demnach ist ein Eingriff zulässig, sofern er gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer. Der *EGMR* hat festgestellt, dass die gesetzliche Grundlage nicht nur abstrakt vorliegen, sondern auch qualitativ eine hinreichende Bestimmtheit und Regelungsdichte vorweisen muss.[102] Folglich müssen die Gesetze zur Überwachung von Individuen einer Vielzahl von Bedingungen genügen: Sie müssen hinreichend klar formuliert sein, sodass für die Bürgerinnen und Bürger ersichtlich ist, unter welchen Voraussetzungen Behörden auf Überwachungsmaßnahmen zurückgreifen können.[103] Ferner muss der möglicherweise von den Überwachungsmaßnahmen betroffene Personenkreis bereits im Gesetz klar abgrenzbar definiert werden.[104] Eine geheime Überwachung der Kommunikation, die vom *EGMR* als „für den Polizeistaat typisch" beschrieben wird,[105] kann zwar durchaus erforderlich sein, um das Interesse einer demokratischen Gesellschaft zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung zu gewährleisten,[106] muss dabei aber auch unbedingt notwendig für den Erhalt demokratischer Einrichtungen sein.[107] Diese unbedingte Notwendigkeit der Maßnahme ist unter zweierlei Gesichtspunkten Voraussetzung: zum einen im Allgemeinen zum Erhalt der demokratischen Einrichtungen, zum anderen im Speziellen zum

[102] *EGMR*, *Malone* v. *Vereiniges Königreich*, Urt. v. 2.8.1984, Rs. 8691/79, Rn. 67, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-57533 (zuletzt abgerufen am 17.12.2018).
[103] *Ebd.*; *EGMR*, *Bykov* v. *Russland*, Urt. v. 10.3.2009, Rs. 4378/02, Rn. 78 f., abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-91704 (zuletzt abgerufen am 17.12.2018).
[104] *EGMR*, *Szabó und Vissy* v. *Ungarn*, Urt. v. 12.1.2016, Rs. 37138/14, Rn. 66, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-160020 (zuletzt abgerufen am 17.12.2018).
[105] *Ebd.*, Rn. 54.
[106] *EGMR*, *Klass u.a.* v. *Deutschland*, Urt. v. 6.9.1978, Rs. 5029/71, Rn. 48, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-57510 (zuletzt abgerufen am 17.12.2018).
[107] *EGMR*, *Szabó und Vissy* v. *Ungarn*, Urt. v. 12.1.2016, Rs. 37138/14, Rn. 54, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-160020 (zuletzt abgerufen am 17.12.2018).

Erlangen der für die Operation notwendigen Informationen.[108] Die Genehmigung der Überwachungsmaßnahme muss von einer politisch von der Exekutive unabhängigen Instanz erfolgen, wenn auch nicht zwingend als Richtervorbehalt ausgestaltet sein.[109] Insbesondere eine nachträgliche Information über die erfolgte Überwachung, verbunden mit der Möglichkeit der richterlichen Überprüfung der Rechtmäßigkeit, ist notwendig, um das Vertrauen der Bürgerinnen und Bürger in den demokratischen Rechtsstaat zu stärken.[110] Etwas anders sieht der *EGMR* dies jedoch bei anlassloser Vorratsdatenspeicherung. Grundsätzlich handele es sich dabei um eine Maßnahme, die vom weiten Ermessensspielraum des Gesetzgebers im Bereich des Schutzes der nationalen Sicherheit gedeckt ist.[111] Zwar müsse auch hier eine unabhängige Kontrolle der Überwachungsmaßnahmen gewährleistet sein, [112] eine spätere Benachrichtigung des betroffenen Individuums über die erfolgte Überwachung sei jedoch ebenso wie ein konkreter Tatverdacht – da dies mit dem Wesen der Vorratsdatenspeicherung nicht vereinbar sei – nicht notwendig.[113]

4. Rechtsschutz

Gemäß Art. 34 EMRK kann der *EGMR* von jeder natürlichen Person mit der Behauptung, in einem in der EMRK verbürgten Recht verletzt zu sein, angerufen werden. Notwendig ist jedoch gemäß Art. 35 Abs. 1 EMRK die vorherige Ausschöpfung aller nationalen Rechtsbehelfe. Eine Besonderheit bei der Geltendmachung einer Verletzung des Rechts auf Privatsphäre ist neben der genannten Notwendigkeit der Möglichkeit einer gerichtlichen Überprüfung, dass die bloße Existenz verdeckter Maßnahmen bzw. einer Gesetzgebung, die verdeckte Maßnahmen erlaubt, für die Klagebefugnis genügt, ohne dass eine unmittelbare Betroffenheit der beschwerdeführenden Person vorliegen muss.[114] Während der *EGMR* in seiner früheren Rechtsprechung noch wenigstens die Darlegung einer begründeten Wahrscheinlichkeit der Überwachung für erfor-

[108] *EGMR*, *Szabó und Vissy* v. *Ungarn*, Urt. v. 12.1.2016, Rs. 37138/14, Rn. 73, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-160020 (zuletzt abgerufen am 17.12.2018).
[109] *Ebd.*, Rn. 75 f.
[110] *Ebd.*, Rn. 78 ff.
[111] *EGMR*, *Big Brother Watch* v. *Vereinigtes Königreich*, Urt. v. 13.9.2018, Rs. 58170/13, 62322/14, 24960/15, Rn. 314 ff., abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-186048 (zuletzt abgerufen am 17.12.2018).
[112] *Ebd.*, Rn. 346 f.
[113] *Ebd.*, Rn. 317.
[114] *EGMR*, *Klass u.a.* v. *Deutschland*, Urt. v. 6.9.1978, Rs. 5029/71, Rn. 34, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-57510 (zuletzt abgerufen am 17.12.2018); *EGMR*, *Szabó und Vissy* v. *Ungarn*, Urt. v. 12.1.2016, Rs. 37138/14, Rn. 33 ff., abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-160020 (zuletzt abgerufen am 17.12.2018).

derlich hielt,[115] lässt er es in der jüngeren Rechtsprechung genügen, dass eine Überwachung nicht ausgeschlossen ist.[116]

Insbesondere im Bereich der anlasslosen bzw. nur an geringe Voraussetzungen geknüpfte (Massen-)Überwachung dürfte die Klagebefugnis also in aller Regel gegeben sein.

II. Art. 7 und Art. 8 der Grundrechtecharta der Europäischen Union; Art. 16 des Vertrages über die Arbeitsweise der Europäischen Union

Das Recht auf Schutz der Privatsphäre findet sich im Primärrecht der Europäischen Union (EU) in einer Vielzahl von Vorschriften. So normiert Art. 7 der Grundrechtecharta der EU (GrCh) ein allgemeines Recht auf Achtung des Privatlebens und der Kommunikation, vergleichbar mit Art. 8 EMRK sowie Art. 17 IPbpR. Mit Art. 8 GrCh besteht sogar ein explizites Recht der Menschen auf Schutz der sie betreffenden personenbezogenen Daten, welches als „Datenschutzrecht" mit seinem besonderen Bezug zum Cyberspace ein Alleinstellungsmerkmal im Vergleich zu dem in der EMRK bzw. im IPbpR verbürgten, allgemeinen Recht auf Privatsphäre hat. Datenschutzrecht und das Recht auf Privatsphäre sind nicht identisch, aber verwandt und habe viele Überschneidungen. So schützt das Datenschutzrecht bspw. jedes personenbezogene Datum, also auch solche Daten, die nicht der Privatsphäre zuzuordnen sind.[117] In Bezug zu Art. 8 GrCh steht Art. 7 GrCh im Bereich des Schutzes personenbezogener Daten, die der Privatsphäre zuzuordnen sind, dementsprechend in Idealkonkurrenz.[118] Die beiden Rechte verstärken sich gegenseitig.[119] Bemerkenswert ist zudem Art. 16 Abs. 1 AEUV, welcher ebenfalls ein Grundrecht auf Datenschutz normiert. Warum eine solche Dopplung des Datenschutzgrundrechts im EU-Primärrecht erfolgte, ist unklar.[120] Beide Rechte sind jedoch deckungsgleich, insbesondere unterliegen sie den gleichen Schranken.[121] Die

---

[115] *EGMR*, *Halford* v. *Verein. Königreich*, Urt. v. 25.6.1997, Rs. 20605/92, Rn. 55 ff., abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-58039
(zuletzt abgerufen am 17.12.2018).
EGMR, *Szabó und Vissy* v. *Ungarn*, Urt. v. 12.1.2016, Rs. 37138/14, Rn. 38, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-160020 (zuletzt abgerufen am 17.12.2018).

[117] Siehe zu den Ähnlichkeiten, aber auch Unterscheidungen ausführlich *Kokott/Sobotta*, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law 2013, S. 222 ff.

[118] *Jarass*, Charta der Grundrechte der EU, 3. Aufl. 2016, Art. 8 Rn. 4; *EuGH*, Urt. v. 8.4.2014, C-293/12, *Digital Rights ./. Ireland*, Rn. 29.

[119] *Jarass* (Fn. 118), Art. 8 Rn. 4; *EuGH*, Urt. v. 8.4.2014, C-293/12, *Digital Rights ./. Ireland*, Rn. 53.

[120] *Kingreen*, in: Callies/Ruffert, EUV/AEUV, 5. Aufl. 2016, Art. 16 AEUV Rn. 3.

[121] *Brühann*, in: v. d. Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 16 AEUV Rn. 30 ff., 37.

nachfolgende Analyse wird sich auf Art. 7 und Art. 8 GrCh konzentrieren, gilt aber entsprechend auch für Art. 16 AEUV.

Zu beachten ist ferner, dass der europarechtliche Datenschutz eine doppelte Zielrichtung verfolgt. So stellt er einerseits einen individualrechtlichen Abwehranspruch des einzelnen Bürgers bzw. der einzelnen Bürgerin gegenüber dem Staat dar und konstituiert eine Schutzpflicht des Staates, andererseits ist Ziel des europäischen Datenschutzes aber auch immer der freie, ungehinderte Datenverkehr innerhalb der EU.[122]

1. Schutzbereich des Art. 7 und Art. 8 GrCh

Art. 7 GrCh ist von seiner gesamten Struktur und seinem Wortlaut stark an Art. 8 Abs. 1 EMRK angelehnt. Statt von „Korrespondenz" wird in der GrCh der Begriff der „Kommunikation" verwendet. Dies soll jedoch keine Änderung des Schutzbereiches bewirken, sondern vielmehr nur den neuen technischen Entwicklungen Rechnung tragen.[123] Ferner kommt die Regelung des Art. 52 Abs. 3 GrCh zum Tragen, nach dem Rechte der Charta, die Rechten der EMRK entsprechen, mindestens den gleichen Schutz bieten. Mithin hat Art. 7 GrCh weitgehend den gleichen Schutzbereich wie Art. 8 EMRK,[124] wobei sich bspw. im Bereich der Vorratsdatenspeicherung ein gesteigertes Schutzniveau unter der GrCh anzudeuten scheint.[125]

Der Schutz personenbezogener Daten nach Art. 8 GrCh umfasst nicht nur Daten aus dem Privat- oder Intimbereich, die also unmittelbar der Privatsphäre zuzuordnen sind, sondern generell sämtliche Daten mit Personenbezug. Es gibt folglich kein belangloses Datum mehr[126] und es kommt auch nicht darauf an, ob eine Information sensiblen Charakter hat oder ob der betroffenen Person durch die Maßnahme Nachteile entstehen.[127] Dies macht deutlich, dass Art. 7 und Art. 8 GrCh zwar im Ergebnis wohl den gleichen Schutzbereich wie Art. 8 EMRK haben – jedenfalls sofern dieser weit ausgelegt wird –, sie aber explizit und unmissverständlich jede Form der personenbezogenen Daten schützen, während bei Art. 8 EMRK erst Gerichte die – in Zeiten von *Big Data* wohl

[122] Siehe Art. 39 EUV sowie Art. 16 Abs. 2 AEUV, die sich jeweils explizit auf den freien Datenverkehr beziehen. Hierzu auch *Frenz*, Handbuch Europarecht IV: Europäische Grundrechte, 2009, Rn. 1357 ff.
[123] Erläuterungen zur GrCh, Amtsblatt der EU v. 14.12.2007, 2007/C 303, S. 2
[124] Ebd., S. 20.
[125] Zu Unterschieden in Bezug auf die Speicherung von Daten von Personen, die keinen Bezug zu Straftaten haben, siehe unten **C. II. 4**.
[126] Die Rechtsprechung des deutschen *BVerfG* zustimmend zitierend *Augsberg*, in: v. d. Groeben/Schwarze/Hatje (Fn. 121), Art. 8 GrCh Rn. 6.
[127] *EuGH*, Urt. v. 8.4.2014, C-293/12, *Digital Rights ./. Ireland*, Rn. 33.

regelmäßig bestehende – Bedeutung für die Privatsphäre des Individuums aufzeigen müssen. Konsequenterweise stellt auch die Speicherung von Metadaten einen Eingriff in Art. 7 und Art. 8 GrCh dar, der bei einer anlasslosen Vorratsdatenspeicherung als besonders schwerwiegend anzusehen ist.[128] Eine massenhafte Speicherung von Inhaltsdaten der Kommunikation würde sogar den absolut geschätzten Wesensgehalt von Art. 7 und Art. 8 GrCh berühren.[129]

Besonders hervorzuheben ist das vom *EuGH* entwickelte „Recht auf Vergessenwerden". In *Google Spain* entschied der *EuGH*, dass sich aus Art. 7 und Art. 8 GrCh ergebe, dass eine Person nicht hinnehmen müsse, dass in den Ergebnislisten der Suchmaschinen Informationen über sie – jedenfalls sofern sie veraltet und nicht mehr von Bedeutung sind – angezeigt werden.[130] Die GrCh entfaltete hierbei eine mittelbare Drittwirkung im Rahmen der Auslegung der strittigen Normen der damals gültigen Datenschutzrichtlinie 95/46/EG. Eine weitere Ausformung der sich aus Art. 7 und Art. 8 GrCh ergebenden Schutzpflicht des Staates ist die am 25.5.2018 gültig gewordene EU-Datenschutzgrundverordnung (DSGVO), die weit auch in das horizontale Verhältnis von Privaten untereinander hineinwirkt. Auf sie wird im Folgenden noch detaillierter eingegangen werden.[131]

2. Überwachung durch unabhängige Behörden nach Art. 16 Abs. 2 S. 2 AEUV

Wenn auch kein subjektives Recht darstellend, ist doch bemerkenswert, dass die Einhaltung des Rechts auf Schutz personenbezogener Daten gemäß Art. 16 Abs. 2 S. 2 AEUV durch eine unabhängige Stelle gewährleistet werden muss. Warum diese Verpflichtung aus Art. 16 AEUV auch die Mitgliedstaaten (Plural: „unabhängige[n] Behörden") trifft, Art. 8 GrCh als Teil des unionsrechtlichen Grundrechtsschutzes dagegen explizit nur die Union verpflichtet (Singular: „unabhängige Stelle"), ist unklar. Im Ergebnis ist dies aber auch nicht von Bedeutung, da das Bestehen der entsprechenden Verpflichtung sowohl für die Mitgliedstaaten als auch für die Union selbst unstrittig ist.[132] Der *EuGH* hat in mehreren Entscheidungen hervorgehoben, dass die politische Unabhängigkeit der Aufsichtsstelle von großer Bedeutung ist und sie deshalb keiner (mitglied-)

[128] *EuGH*, Urt. v. 8.4.2014, C-293/12, *Digital Rights ./. Ireland*, Rn. 35 ff.
[129] *Ebd.*, Rn. 38 f.
[130] *EuGH*, Urt. v. 13.5.2014, C-131/12, *Google Spain ./. Spanien*, Rn. 99.
[131] Siehe unten **C. III.**
[132] *Kingreen*, in: Callies/Ruffert (Fn. 120), Art. 8 GrCh Rn. 18.

staatlichen Rechts- oder Fachaufsicht unterstellt sein darf, aber natürlich trotzdem der gerichtlichen Kontrolle unterliegt.[133]

3. Anwendungsbereich

Die Besonderheit des EU-Grundrechtsschutzes liegt darin, dass er nicht konsequent auf alle unter ihm liegenden Ebenen durchschlägt, sondern unmittelbar nur die Organe der Union sowie gemäß Art. 51 Abs. 1 GrCh die Mitgliedstaaten bei der Durchführung von Unionsrecht bindet.[134] Da die Europäische Union auch nicht über einen Geheimdienst oder einen eigenen Polizeiapparat verfügt, stellen sich viele der klassischen Fragen bei der Gewährleistung des Rechts auf Schutz der Privatsphäre des Individuums, in welches oftmals durch geheime Überwachungsmaßnahmen staatlicher Sicherheitsapparate eingegriffen wird, nicht auf EU-Ebene. Die umfangreichen sekundärrechtlichen Regelungen zum Datenschutz führen aber dazu, dass bspw. nationale Regelungen zur Vorratsdatenspeicherung in den Bereich der Durchführung von Unionsrecht fallen und der *EuGH* in der Vergangenheit bereits entschied, dass diese nicht mit Unionsrecht vereinbar seien.[135] Auch die deutsche Vorratsdatenspeicherung, die derzeit ausgesetzt ist[136] und vor dem *Bundesverfassungsgericht* angegriffen wird, soll nach dem Willen der Bundesregierung vom *EuGH* auf ihre Europarechtskonformität überprüft werden.[137]

Der generelle Anknüpfungspunkt ist also nicht – wie bei der EMRK und dem IPbpR – die Frage der Hoheitsgewalt, sondern ob eine Handlung eines Mitgliedstaates im Rahmen der Durchführung von Unionsrecht vollzogen wird. Dementsprechend sind die Staaten auch bei extra-territorialen Akten, sofern sie einen Vollzug von Unionsrecht darstellen, an die GrCh gebunden.[138]

---

[133] *EuGH*, Urt. v. 9.3.2010, C-518/07, *Kommission ./. Deutschland*, Rn. 42.
[134] *Jarass* (Fn. 118), Art. 8 Rn. 3.
[135] *EuGH*, Urt. v. 21.12.2016, C-203/15, *Tele2 Sverige ./. Schweden*, Rn. 73 ff., 106, 125.
[136] *Bundesnetzagentur*, Verkehrsdatenspeicherung: Mitteilung zur Speicherverpflichtung nach § 113b TKG, Stand: 28.6.2017, abrufbar unter: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html (zuletzt abgerufen am 17.12.2018).
[137] *Steiner*, Überwachung: Regierung will Vorratsdatenspeicherung vom *EuGH* prüfen lassen, Deutschlandfunk, 31.8.2018, abrufbar unter: https://www.deutschlandfunk.de/ueberwachung-regierung-will-vorratsdatenspeicherung-vom.1773.de.html?dram:article_id=426891 (zuletzt abgerufen am 17.12.2018).
[138] So auch *Jarass* (Fn. 118), Art. 51 Rn. 39 m. w. N.

4. Schranken

Auch im Europarecht wird das Grundrecht auf Achtung des Privatlebens bzw. des Schutzes personenbezogener Daten nicht schrankenfrei gewährt. So kann gemäß Art. 52 Abs. 1 GrCh in die in der Charta garantierten Rechte und Freiheiten auf Basis einer gesetzlichen Grundlage eingegriffen werden, sofern der Eingriff erforderlich ist und dem Gemeinwohl dient bzw. ein Erfordernis für Schutz der Rechte anderer darstellt. Eingriffe in Art. 7 und Art. 8 GrCh müssen dabei – gemäß Art. 52 Abs. 3 GrCh in Anlehnung an die Schranken von Art. 8 EMRK – auf das absolut Notwendige beschränkt werden.[139] Anders als der *EGMR*[140] hat der *EuGH* jedoch entschieden, dass eine pauschale, anlasslose Speicherung, die keinerlei Differenzierung zwischen Personen vornimmt, die – wenn auch nur mittelbar oder entfernt – im Zusammenhang mit einer Straftat stehen, und solchen, die als vollkommen unverdächtig einzustufen sind, nicht mit den in Art. 7 und Art. 8 GrCh garantierten Rechten vereinbar ist.[141]

5. Rechtsschutz

Grundsätzlich existiert keine direkte Klagemöglichkeit für einzelne Bürgerinnen und Bürger vor dem *EuGH*. Fragen der Auslegung oder der Gültigkeit von Unionsrechtsakten bzw. nationalen Gesetzen, die eine Durchführung von Unionsrecht i. S. d. Art. 51 Abs. 1 GrCh darstellen, können bzw. müssen in Verfahren vor den nationalen Gerichten der Mitgliedstaaten der EU gemäß Art. 267 AEUV an den *EuGH* gestellt werden. Dieses Verfahren hat inzwischen eine überragende Bedeutung für den Individualrechtsschutz gewonnen.[142]

III. Datenschutzgrundverordnung der Europäischen Union

Der Zweck der DSGVO ist nach Art. 1 zum einen der Schutz der Grundrechte und Grundfreiheiten, zum anderen aber auch der freie Verkehr von Daten. Sie ist dabei gemäß Art. 2 Abs. 2 lit. d sachlich nicht anwendbar auf den äußerst grundrechtssensiblen Bereich der Verhütung, Ermittlung und Verfolgung von Straftaten.[143] Dieser Bereich wird stattdessen über eine eigene Richtlinie[144] unter Beachtung der einschlägigen in der GrCh garantierten Rechte reguliert.[145] Dies

[139] *EuGH*, Urt. v. 7.11.2013, C-473/12, *IPI ./. Englebert*, Rn. 39; Urt. v. 6.12.2008, C-73/07, *Satakunnan Markkinapörssi und Satamedia ./. Tietosuojavaltuutettu*, Rn. 56.
[140] Siehe hierzu oben **C. I. 3**.
[141] So bereits in *EuGH*, Urt. v. 8.4.2014, C-293/12, *Digital Rights ./. Ireland*, Rn. 57 f., explizit später im Urt. v. 21.12.2016, C-203/15, *Tele2 Sverige ./. Schweden*, Rn. 105 ff., 106, 125.
[142] *Wegener*, in: Callies/Ruffert (Fn. 120), Art. 267 AEUV Rn. 1.
[143] Siehe hierzu auch Erwägungsgrund 19 der DSGVO.
[144] RL2016/680/EU des Europäischen Parlaments und des Rates v. 27.4.2016.
[145] *Ernst*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 2 DSGVO Rn. 22 f.

zeigt, dass die DSGVO zwar sowohl einfachrechtlicher Ausfluss der abwehrrechtlichen Dimension als auch der Schutzpflicht der Grundrechte auf Privatsphäre und Datenschutz ist, der Schwerpunkt wohl aber bei letzterem liegt. Die Regulierung des horizontalen Verhältnisses Privater untereinander wird durch die DSGVO weitgehend abschließend[146] einheitlich innerhalb der EU betrieben, ihr Anwendungsbereich im Verhältnis Staat zu Bürger nimmt jedoch ausgerechnet den Strafverfolgungsbereich, wo besonders intensive Eingriffe zu befürchten sind, aus und unterwirft diesen einem anderem Regelungsregime.

Der Anknüpfungspunkt zur Eröffnung des Anwendungsbereichs hat im Bereich der Datenverarbeitung im Unionsrecht zwei Ausprägungen. Die Verordnung findet gemäß Art. 3 Abs. 1 DSGVO unabhängig vom Ort der Datenverarbeitung Anwendung, sofern sie im Rahmen der Tätigkeit eines in der Union ansässigen Verantwortlichen oder Auftragsverarbeiters[147] erfolgt. Art. 3 Abs. 2 DSGVO konstituiert zudem, dass die Verordnung auch immer dann anwendbar ist, wenn nicht-europäische Verantwortliche oder Auftragsverarbeiter Waren oder Dienstleistungen in der Union anbieten oder das Verhalten von Personen in der Union beobachten. Hier lässt sich hier klar das Konzept eines *factual links*[148] zwischen Eingriff (ggf. durch Private) und betroffener Person erkennen. Sobald es also einen Bezugspunkt zur Europäischen Union gibt, greift die Verordnung als Ausprägung der menschenrechtlichen Schutzpflicht und reguliert den durch die Verarbeitung personenbezogener Daten stattfindenden Eingriff in Art. 7 und Art. 8 GrCh.

Inhaltlich kodifiziert die Verordnung sowohl Grundsätze für die Verarbeitung personenbezogener Daten[149] als auch den Einwilligungsvorbehalt der betroffenen Person als eine der Voraussetzungen unter denen die generell unzulässige Verarbeitung von Daten zulässig sein kann.[150] Auch das vom *EuGH* entwickelte „Recht auf Vergessenwerden" wurde in Art. 17 der Verordnung explizit aufgenommen.

---

[146] Zur Ausnahme vom Grundsatz der abschließenden Regelung siehe bspw. die Öffnungsklausel des Art. 85 Abs. 2 DSGVO.
[147] Zu den Legaldefinitionen siehe Art. 4 Nr. 7, 8 DSGVO.
[148] Siehe dazu auch oben **B. II. 2.** *d)* bzw. **B. II. 2.** *f)*.
[149] Art. 5 DSGVO, u. a. die Rechtmäßigkeit und Zweckbindung der Daten sowie Datenminimierung und einen Anspruch auf Richtigkeit der Daten.
[150] Art. 6 DSGVO, neben der Einwilligung kommt u. a. auch eine Rechtfertigung nach einer Abwägung zwischen den berechtigten Interessen der datenverarbeitenden Stelle bzw. eines Dritten und denen der betroffenen Person in Betracht (Art. 6 Abs. 1 lit. f). Die Einwilligung kann gemäß Art. 7 Abs. 3 DSGVO jederzeit widerrufen werden.

Insgesamt lässt sich sagen, dass es sich bei der DSGVO um das weltweit wohl ausgefeilteste und weitgehendste Datenschutzrecht handelt, das bisher kodifiziert wurde. Insbesondere aufgrund des weiten Anwendungsbereichs, dem mindestens die rund 511 Millionen Einwohnerinnen und Einwohner der EU[151] unterfallen, entfaltet es eine enorme Wirkung für den Schutz der Privatsphäre im Cyberspace im horizontalen Verhältnis Privater untereinander.

D. Fazit

Das Recht auf Schutz der Privatsphäre im Cyberspace ist *de jure* sowohl im internationalen als auch im regionalen Völkerrecht umfassend gegeben.

Für den internationalen Menschenrechtsschutz durch den IPbpR hat der UN-Menschenrechtsausschuss in seinen *General Comments* den Schutzbereich des Rechts auf Privatsphäre bzw. auf Schutz der Korrespondenz schon früh so weit gezogen, dass die Subsumtion von Sachverhalten aus dem digitalen Zeitalter unter dieses Recht grundsätzlich keine besonderen Schwierigkeiten bereitet. Problematisch bleibt die Frage des Anwendungsbereiches. Auch wenn sich – bis auf wenige Ausnahmen – die Wissenschaft und auch die Generalversammlung einig zu sein scheint, dass im Cyberspace keine Schutzlücke für die Privatsphäre aufgerissen werden darf, nur weil sich Überwacher, überwachte Person und das überwachte Objekt – die Daten – nicht am gleichen Ort befinden, ist derzeit noch unklar, wie die Weitung des Anwendungsbereichs dogmatisch begründet wird.

Trotz der im Vergleich guten rechtlichen Position, ist die Rechtsdurchsetzung im internationalen Kontext mangelhaft. Weltweit gibt es – politisch gerechtfertigt durch einen globalen *War on Terror* – umfassende Überwachungsprogramme durch Geheimdienste und Sicherheitsbehörden. In Ermangelung eines Rechtsprechungsorgans, das den IPbpR rechtsverbindlich und authentisch für die Parteien auslegt, können sich die Staaten unproblematisch auf eine eigene, restriktive Auslegung zurückziehen und haben – außer Kritik an ihrer Position – keine Konsequenzen zu befürchten.[152]

---

[151] *Eurostat*, Bevölkerung am 1. Januar, Stand 2017, abrufbar unter: http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&plugin=1&language=de&pcode=tps00001 (zuletzt abgerufen am 17.12.2018).

[152] Siehe als Beispiel für die durchaus harsche Ablehnung solcher Kritik – hier in Bezug auf die extra-territoriale Anwendung des IPbpR: *US-Bundesregierung* (Fn. 35), S. 754: „*These non-binding authorities* [the Human Rights Committee with its General Comment and the ICJ with its advisory opinion] *cannot rewrite the binding obligations undertaken and consented to by States Parties upon ratification of the ICCPR. "Soft Law" cannot amend hard law, as much as some might wish it were so*."

Umso bedeutsamer ist daher der Bereich des regionalen Menschenrechtsschutzes, der insbesondere in Europa deutlich wirkmächtiger ist. Mit Spannung ist hierbei das Verhältnis von *EGMR* und *EuGH* zu beobachten: In der Frage der anlasslosen, massenhaften Überwachung der Einwohnerinnen und Einwohner europäischer Staaten durch die Vorratsdatenspeicherung hat der sich der *EuGH* zunächst für einen umfassenden Grundrechtsschutz stark gemacht,[153] während die darauffolgende *Big Brother Watch*-Entscheidung des *EGMR* zurückhaltender wirkt.[154] Die Entscheidungen des *EuGH* zu den derzeit anhängigen Vorabentscheidungsverfahren[155] hinsichtlich nationaler Gesetzgebung zur Vorratsdatenspeicherung wird deshalb wegweisend für die Frage sein, welches Gericht für den Schutz der Bürgerinnen und Bürger Europas zukünftig eine größere Rolle spielen wird.

Grund zum Optimismus verleiht die Aufmerksamkeit, die das Thema der digitalen Überwachung in der Diplomatie und den Internationalen Organisationen erhält. Der Bericht der Hohen Kommissarin zum Recht auf Privatsphäre im digitalen Zeitalter und die Einsetzung des Sonderberichterstatters zeigen, dass es ernst genommen wird.

Trotzdem besteht noch Handlungsbedarf:

Der UN-Menschenrechtsausschuss könnte einen *General Comment* zur Anwendbarkeit der Menschenrechte im Cyberspace veröffentlichen,[156] der klarstellende Wirkung entfalten würde. Denkbar wäre auch die Einholung eines IGH-Gutachtes zu dieser Rechtsfrage.

Das in der EU-Grundrechtecharta verbürgte Recht auf den Schutz personenbezogener Daten sollte explizit auch in internationale Menschenrechtsverträge, bspw. durch Fakultativprotokolle, aufgenommen werden.

Die Staaten müssen ihre menschenrechtlichen Schutzpflicht ernster nehmen. Hierzu gehört die kritische Überprüfung geheimdienstlicher Kooperationen,[157]

[153] Siehe dazu oben **C. II. 1.** und **3.**
[154] Siehe dazu oben **C. I. 3.**
[155] Zur Vorlage des *belgischen Verfassungsgerichtes* siehe *Verbruggen/Royer/Severijns*, Reconsidering the blanket-data-retention-taboo, for human rights' sake?, European Law Blog, 1.10.2018, abrufbar unter: https://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake (zuletzt abgerufen am 17.12.2018); zur evtl. Vorlage durch das *BVerfG* siehe *Steiner* (Fn. 137).
[156] So auch *Peters* (Fn. 29), S. 177 f.
[157] Auch wenn der *EGMR* grundsätzlich das Teilen von Informationen unter Geheimdiensten als zulässig erachtet hat, so hat er doch betont, dass in dem Empfangen solcher Informationen ein Eingriff in das Recht auf Privatsphäre liege und der empfangen-

aber auch die Regulierung des privaten Datenmarkts, insbesondere im Kontext der zunehmenden Auswertung von *Big Data*. Die DSGVO ist hierbei ein erster Meilenstein, der als Vorbild bei der Einführung ähnlicher Instrumente in anderen Regionen, bspw. durch völkerrechtliche Abkommen, dienen kann.

Die Bedeutung des Internets für die Freiheit des Individuums kann nicht überschätzt werden. Der Cyberspace ist ein Ort der Kommunikation, der Information und der Selbstverwirklichung. Wird das Internet aber flächendeckend überwacht, so wird die Gesellschaft flächendeckend überwacht und die Axt an die Grundfesten demokratischer Freiheiten gelegt.

de Staat sicherstellen muss, das die vorherige Sammlung nicht unter Missachtung menschenrechtlicher Standards durchgeführt wurde: *EGMR*, *Big Brother Watch* v. *Vereinigtes Königreich*, Urt. v. 13.9.2018, Rs. 58170/13, 62322/14, 24960/15, Rn. 421-424, abrufbar unter: http://hudoc.echr.coe.int/eng?i=001-186048
(zuletzt abgerufen am 17.12.2018).