Sachstand

Völkerrechtliche Aspekte der Zulässigkeit geheimdienstlicher Aktivitäten

Völkerrechtliche Aspekte der Zulässigkeit geheimdienstlicher Aktivitäten

Aktenzeichen:	WD 2 - 3000 - 094/19
Abschluss der Arbeit:	9. September 2019
Fachbereich:	WD 2: Auswärtiges, Völkerrecht, wirtschaftliche Zusammenarbeit und Entwicklung, Verteidigung, Menschenrechte und humanitäre Hilfe

Inhaltsverzeichnis

1. Einführung

Die Fragestellung des Auftraggebers hat u.a. Aspekte der völkerrechtlichen Bewertung geheimdienstlicher Aktivitäten zum Gegenstand. Vor diesem Hintergrund wird zunächst die Frage behandelt, inwieweit ausländische Spionagehandlungen durch völkerrechtliche Regelungen generell verboten sind. Hierauf aufbauend werden die völkerrechtlichen Grenzen geheimdienstlicher Aktivitäten, die sich aus dem Diplomatenrecht und Menschenrechten ergeben, aufgezeigt. Das vorliegende Gutachten beschränkt sich dabei auf völkerrechtliche Aspekte und beschäftigt sich nicht mit einschlägigen nationalen strafrechtlichen oder verfassungsrechtlichen Fragen.

2. Völkerrechtliche Regelungen zu geheimdienstlichen Aktivitäten

Spionage in Friedenszeiten ist im Völkerrecht nicht durch speziellen Normen geregelt. Sie ist weder ausdrücklich erlaubt, noch durch ein völkerrechtliches Abkommen explizit verboten. Für Spionage in Kriegszeiten enthält Artikel 46 des ersten Zusatzprotokolls zu den Genfer Abkommen[1] eine spezielle Regelung, wonach Spionen unter bestimmten Voraussetzungen der Status als Kriegsgefangene versagt wird.[2]

2.1. Abkommen

Ein völkerrechtliches Spionageverbot kann sich aus zwischenstaatlichen Verträgen ergeben, durch die sich Vertragsparteien verpflichten, keine Abhörmaßnahmen oder sonstige Spionagetätigkeiten gegenüber ihrem Vertragspartner vorzunehmen. Ansatzweise existiert ein derartiges Abkommen in Gestalt der britisch - US-amerikanischen Fernmeldeaufklärungsvereinbarung vom 5. März 1946 (*British-U.S. Communication Intelligence Agreement*).[3] Da dieser Vereinbarung später Australien, Kanada und Neuseeland ebenfalls beigetreten sind, wird auch von der sog. „Fünf-Augen-Allianz“ gesprochen. Ein ausdrückliches Spionageverbot enthält die Vereinbarung allerdings nicht. Das Abkommen regelt vielmehr den umfassenden Austausch von geheimdienstlichen Informationen der betroffenen Staaten untereinander, so dass ein gegenseitiges Ausspähen unter diesen Voraussetzungen nicht mehr nötig erscheint. Die Vereinbarung ist außerdem eher als politische Abmachung – als *Gentlemen's Agreement* oder *Memorandum of Understanding* –

1 Zusatzprotokoll vom 8. Juni 1977 zu den Genfer Abkommen, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/INTRO/470.

2 Weitergehend Schaller/Spies, in: Wolfrum (Hrsg.), MPEPIL, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e295?rskey=mPQ0kP&result=2&prd=OPIL.

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

zwischen den jeweiligen Geheimdiensten denn als völkerrechtlich verbindlicher Vertrag zu qualifizieren.[4] Im Allgemeinen sind die Staaten eher zurückhaltend, wenn es um den Abschluss von sog. *No-Spy*-Abkommen geht. Regelmäßig haben sie kein Interesse daran, ihren Handlungsspielraum in diesem sensiblen Bereich einzuschränken. Weitere *No-Spy*-Abkommen sind daher nicht bekannt.[5] Anlässlich der NSA-Affäre stand die Frage der Verhandlung eines entsprechenden Abkommens zwischen Deutschland und den Vereinigten Staaten im Raum, das schließlich aber nicht zustande gekommen ist.[6]

2.2. VN-Resolution Nr. 68/167 „Recht auf Privatsphäre im digitalen Zeitalter“

Im Zusammenhang mit der NSA-Affäre hat die VN-Generalversammlung auf Initiative Deutschlands und Brasiliens am 18. Dezember 2013 die Resolution Nr. 68/167 „Recht auf Privatsphäre im digitalen Zeitalter“ verabschiedet.[7] In der Resolution wird das Recht auf Privatsphäre bekräftigt (Art. 1 der Resolution) und es werden alle Staaten aufgerufen, ihre Verfahren, Praktiken und Rechtsvorschriften in Bezug auf die Überwachung von Kommunikation im Lichte der einschlägigen Menschenrechtsverpflichtungen zu überprüfen (Art. 4 lit. c der Resolution). Sie werden außerdem dazu aufgerufen, Maßnahmen zu ergreifen, um Verstöße gegen das Recht auf Privatsphäre zu beenden und die Voraussetzungen für dessen Schutz zu schaffen (Art. 4 lit. b der Resolution). Im Zusammenhang mit dieser Resolution hat die VN-Generalversammlung veranlasst, dass der VN-Hochkommissar für Menschenrechte Berichte zur Förderung und zum Schutz des Rechts auf Privatsphäre im digitalen Zeitalter vorlegt.[8] Mit der Resolution Nr. 28/16 hat der VN-Menschenrechtsrat darüber hinaus im April 2015 einen Sonderberichterstatter für das Recht auf Privatsphäre (*Special Rapporteur on the right to privacy)*[9] für ein Mandat von drei Jahren eingesetzt,

---

4 Talmon, Das Abhören der Kanzlerhandys und das Völkerrecht, BRJ 01/2014, S. 7ff., https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Institute/Voelkerrecht/Dokumente_fuer_Webseite/BRJ_01_2014.pdf, S. 7, siehe auch die Ausarbeitung des Wissenschaftlichen Dienstes „Gewinnung von Telekommunikationsinformationen durch ausländische Nachrichtendienste aus völkerrechtlicher Sicht“, WD 2 – 3000 – 083/13, 11. November 2013, https://sehrgutachten.de/bt/wd2/083-13-gewinnung-von-telekommunikationsinformationen-durch-auslaendische-nachrichtendienste-aus-voelkerrechtlicher-sicht.

5 So auch Schaller, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP Berlin, Oktober 2014, S. 11, file://na07-jkh-fs01/u_daten$/wd2-pc-01-ma01/Dokumente/Geheimdienste/2014_S18_slr.pdf.

6 https://www.deutschlandfunk.de/no-spy-abkommen-es-gab-da-jede-menge-falsche-erwartungen.694.de.html?dram:article_id=274640; siehe weitergehend zu der Frage, ob ein solches Abkommen sinnvoll und realistisch wäre: Talmon, (Fn.4).

7 UN General Assembly, Resolution 68/167, The Right to Privacy in the Digital Age, 18. Dezember 2013, https://undocs.org/en/A/RES/68/167.

8 Report A/HRC/39/29, 39th session of the Human Rights Council, September 2018, https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx.

9 Special Rapporteur on the right to privacy, https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

das zuletzt am 9. April 2018 verlängert wurde. Seine Aufgabe besteht darin, über mögliche Verletzungen des Rechts auf Privatsphäre, insbesondere auch im Zusammenhang mit den Herausforderungen der neuen Technologien, zu berichten.[10]

Die Resolution Nr. 68/167 ist zwar als Resolution der VN-Generalversammlung rechtlich nicht verbindlich[11] und begründet daher kein eigenständiges völkerrechtliches Verbot geheimdienstlicher Aktivitäten zum Schutz des Rechts auf Privatsphäre.[12] Sie hat aber durchaus politisches und moralisches Gewicht und macht gemeinsam mit den skizzierten Entwicklungen deutlich, dass das Recht auf Privatsphäre im digitalen Zeitalter seit der NSA-Affäre verstärkt in das Bewusstsein der Staaten gerückt ist. Auch wenn Spionagetätigkeiten als solche nicht explizit verboten sind, so signalisieren die Staaten dennoch ihre Bereitschaft, den Schutz und die Durchsetzung des Rechts auf Privatsphäre effektiver gestalten zu wollen.

2.3. Völkergewohnheitsrecht

Auch im Völkergewohnheitsrecht hat sich bislang keine Norm herausgebildet, nach der Spionage per se verboten ist.[13] Das bedeutet im Umkehrschluss allerdings nicht, dass Spionage völkergewohnheitsrechtlich anerkannt und zulässig ist.[14] Auch ohne spezielle völkerrechtliche Regelungen oder bilaterale Abkommen müssen die Staaten bei geheimdienstlichen Aktivitäten die allgemeinen völkerrechtlichen Prinzipien und Regelungen, wie beispielsweise das Diplomaten- und Konsularrecht, respektieren und ihre Verpflichtungen aus internationalen und regionalen Menschenrechtsabkommen einhalten.

---

10 OHCHR, The Right to Privacy in the Digital Age, https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

11 Siehe weitergehend Dörr in: Ipsen, Völkerrecht, 7. Auflage, 2018, § 20 Rn. 2., § 21 Rn. 8.

12 Vgl. weitergehend Talmon (Fn. 4), S. 11.

13 So Schaller, (Fn. 5), S. 11.

14 Peters, Surveillance without borders? The unlawfulness of the NSA-Panopticum, Part I and II, EJIL: Talk, November 2013, http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsapanopticon-part-i/ sowie Peters, „Es gibt kein explizites Verbot der Spionage. Aber das heißt nicht, dass sie erlaubt ist", Verfassungsblog 2013, https://verfassungsblog.de/es-gibt-kein-explizites-verbot-spionage-aber-heisst-nicht-dass-erlaubt-ist/.

3. Völkerrechtliche Grenzen von Spionagetätigkeiten

3.1. Allgemeine völkerrechtliche Prinzipien

Bei geheimdienstlichen Aktivitäten, insbesondere auch im sog. Cyberkontext, können verschiedene, in der Charta der Vereinten Nationen (VN-Charta) [15] verankerte Prinzipen, wie beispielsweise die staatliche Souveränität, die territoriale Integrität, das Interventionsverbot oder das Gewaltverbot, betroffen sein.[16]

Bei der völkerrechtlichen Bewertung von geheimdienstlichen Aktivitäten ist zwischen Überwachungsmaßnahmen, welche direkt vom ausländischen Territorium aus betrieben werden (sog. Fernaufklärung) und geheimdienstlichen Tätigkeiten vom Territorium des ausgespähten Staates aus zu unterscheiden.

Die bloße Fernaufklärung vom Territorium des ausländischen Staates aus wird grundsätzlich nicht als völkerrechtswidrig bewertet.[17] Fernaufklärung ohne physische Präsenz im Inland stellt dabei nach wohl überwiegender Ansicht keinen unzulässigen Eingriff in die inneren Angelegenheiten des überwachten Staates dar.[18] Der Europäische Gerichtshof für Menschenrechte (EGMR) hat im Jahr 2006 in einer Entscheidung gegen Deutschland festgestellt, dass bei der internationalen Überwachung des drahtlosen Fernmeldeverkehrs durch den deutschen Bundesnachrichtendienst in Form des Abhörens von Telefonaten im Ausland, die über Satellit oder Richtfunkstrecken abgewickelt werden, kein Verstoß gegen die völkerrechtlich geschützte territoriale Souveränität anderer Staaten vorliegt, soweit die vom ausländischen Gebiet ausgesandten Funksignale von Deutschland aus überwacht und abgefangen werden.[19]

Im Bereich der Cyberspionage hat sich noch kein Konsens im Völkerrecht herausgebildet, ob das heimliche Eindringen in geschützte IT-Systeme und Netzwerke zu Spionagezwecken gegen das völkerrechtliche Interventionsverbot verstößt.[20] Hierbei wird aber überwiegend die Ansicht vertreten, dass es bei geheimdienstlichen Cyberaktivitäten an dem interventionstypischen Zwangselement fehle und das Interventionsverbot daher nicht verletzt sei.[21]

---

15 Charta of the United Nations, 26. Juni 1945, https://www.un.org/en/charter-united-nations/, deutsche Fassung: https://www.unric.org/de/charta.

16 Siehe weitergehend, Schaller (Fn. 5) S. 7 ff.; Peters (Fn. 14).

17 Vgl. Talmon (Fn. 3), S. 10.

18 So auch Ausarbeitung des Wissenschaftlichen Dienstes „Gewinnung von Telekommunikationsinformationen durch ausländische Nachrichtendienste aus völkerrechtlicher Sicht“, WD 2-3000-083/13, (Fn. 4), S. 6.

19 EMGR, *Weber and Saravia ./. Germany*, Entscheidung vom 29. Juni 2006, Nr. 54934/00.

20 *Ibid.*, S. 12 m.w.N.

21 Peters, (Fn. 14).

3.2. Wiener Übereinkommen über diplomatische Beziehungen

Bei geheimdienstlichen Tätigkeiten mit Territorialbezug ist für deren völkerrechtliche Bewertung insbesondere das Wiener Übereinkommen über diplomatische Beziehungen (WÜD)[22] von Bedeutung. Dieses beinhaltet zwar kein ausdrückliches Spionageverbot für Mitglieder des diplomatischen Personals im Empfangsstaat, setzt ausländischen geheimdienstlichen Aktivitäten aber gewisse Schranken. So sieht Artikel 3 Abs. 1 lit. d WÜD vor, dass es unter anderem Aufgabe einer diplomatischen Mission sei, „sich mit allen rechtmäßigen Mitteln über Verhältnisse und Entwicklungen im Empfangsstaat zu unterrichten und darüber an die Regierung des Entsendestaats zu berichten." Die Nachrichtengewinnung und Berichterstattung gehören damit zu den Kernaufgaben der diplomatischen Mission. Wie sich bereits aus dem Wortlaut des Artikel 3 Abs. 1 lit. d WÜD ergibt, muss diese aber mit „rechtmäßigen Mitteln" erfolgen. Die Grenze zwischen rechtmäßigen Aktivitäten der Beobachtung und Information und unrechtmäßigen Aktivitäten ist zum Teil nur schwer zu treffen. Nachrichtendienstliche Tätigkeiten und Abhörmaßnahmen, die z.B. in Deutschland einen Straftatbestand erfüllen (wie beispielsweise das heimliche Abhören von Telefongesprächen oder das Ausspähen von Daten gemäß §§ 201, 202a, 202b StGB sowie geheimdienstliche Agententätigkeiten im Sinne des § 99 StGB), erfolgen aber nicht mit rechtmäßigen Mitteln im Sinne der Vorschrift.[23]

Art. 41 Abs. 1 WÜD sieht außerdem die Pflicht vor, die Gesetze des Empfangsstaates zu beachten:

> Alle Personen, die Vorrechte und Immunitäten genießen, sind unbeschadet derselben verpflichtet, die Gesetze und anderen Rechtsvorschriften des Empfangsstaates zu beachten. Sie sind ferner verpflichtet, sich nicht in dessen innere Angelegenheiten einzumischen.

Die Verpflichtung zur Beachtung der innerstaatlichen Gesetze ist grundsätzlich umfassend zu verstehen, so dass die bevorrechtigten Personen an das Recht des Empfangsstaates genauso gebunden sind wie nichtprivilegierte Bürger.[24]

Artikel 41 Abs. 3 WÜD sieht darüber hinaus vor:

> Die Räumlichkeiten der Mission dürfen nicht in einer Weise genutzt werden, die unvereinbar ist mit den Aufgaben der Mission, wie sie in diesem Übereinkommen, in anderen Regeln des allgemeinen Völkerrechts oder in besonderen, zwischen dem Entsendestaat und dem Empfangsstaat in Kraft befindlichen Übereinkünften niedergelegt ist.

Die Verpflichtung der Auslandsvertretung, ihre Räumlichkeiten nur für diplomatische Aufgaben zu nutzen, nimmt Bezug auf Art. 3 WÜD, der die Aufgaben der diplomatischen Mission definiert. Eine Nutzung der Räumlichkeiten der Auslandsvertretung zu Spionagezwecken, die nicht der

---

22 Wiener Übereinkommen über diplomatische Beziehungen vom 18.4.1961, BGBl. 1964 II, S. 959.

23 Oelfke, in: WÜD Kommentar, Wagner, Raasch, Pröpstl (Herausgeber), 2018, S. 67; WD 2-3000-083/13 (Fn. 4), S. 9. Zu den strafrechtlichen Aspekten siehe im Einzelnen WD 7- 3000 -126/19 vom 28. August 2019.

24 Oelfke (Fn. 23), S. 325.

Nachrichtengewinnung und Berichterstattung mit rechtmäßigen Mitteln im Sinne des Art. 3 Abs. 1 lit. d WÜD entsprechen, stellt damit eine Verletzung des Diplomatenrechts dar.

Soweit deutsche Staatsbürger folglich von einer Botschaft aus ohne ihr Einverständnis überwacht und abgehört werden und diese Tätigkeiten gegen deutsche Gesetze verstoßen, stellt sich dieses Verhalten des ausländischen Staates als völkerrechtswidrig dar.

Als Reaktionsmöglichkeit auf mögliche Verstöße gegen das Diplomatenrecht, kann der Empfangsstaat u.a. jederzeit und ohne Angabe von Gründen, ein Mitglied des diplomatischen Personals zur *persona non grata* erklären (vgl. Artikel 9 Abs. 1 WÜD). In diesen Fällen hat der Entsendestaat die betreffende Person entweder abzuberufen oder ihre Tätigkeit bei der Mission zu beenden (Art. 9 Abs. 1 S. 2 WÜD).[25]

3.3. Menschenrechtliche Verpflichtungen

Regionale und internationale Menschenrechtsabkommen garantieren das Recht des Einzelnen auf Schutz seiner Privatsphäre vor rechtswidrigen und willkürlichen staatlichen Eingriffen. Bei geheimdienstlichen Aktivitäten müssen die Staaten u.a. auch ihre Verpflichtungen aus internationalen Menschenrechtsabkommen einhalten.[26] Als Privatpersonen genießen auch deutsche Politiker und Amtsträger den Schutz internationaler Menschenrechtsabkommen. Die Vertragsparteien sind jedoch grundsätzlich nur denjenigen Personen zum Schutz verpflichtet, die sich in ihrem Gebiet befinden oder ihrer Herrschaftsgewalt unterstehen.[27] Daher stellt sich bei der Bewertung ausländischer Spionagetätigkeiten am Maßstab von Menschenrechtsverpflichtungen regelmäßig die Frage, inwieweit der ausländische Staat extraterritorial bei seiner Tätigkeit an das jeweilige Menschenrechtsabkommen gebunden ist. In der Völkerrechtswissenschaft wird die Bindung an Menschenrechte zumindest dann bejaht, wenn es sich um Akte handelt, die von diplomatischen oder konsularischen Mandatsträgern des Staates auf ausländischem Boden begangen werden.[28]

Aus verfassungsrechtlicher Sicht[29] ist schließlich insbesondere auch die Frage von Bedeutung, inwieweit Deutschland grundrechtliche Schutzpflichten gegenüber seinen eigenen Staatsangehörigen vor dem Zugriff durch ausländische Spionagetätigkeiten hat. Staatliche Schutzpflichten können sich dabei aus Art. 10 GG sowie aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG

---

25 Siehe zu weitergehenden Reaktionsmöglichkeiten Oelfke (Fn. 23), S. 93 ff.; WD 2-3000-083/13 (Fn. 4), S. 11.

26 Siehe weitergehend zu dieser Problematik WD 2-3000-083/13 (Fn. 4), S. 14 ff.

27 Siehe diesbezüglich Art. 2 Abs. 1 IPbpR, Art. 1 EMRK stellt auf die „ihrer Hoheitsgewalt unterstehenden Personen ab“; Vgl. zum Streitstand Talmon (Fn.4), S. 10; Peters, a.a.O. (Fn. 14).

28 Wenzel, Human Rights, Treaties, Extraterritorial Application and Effects, in: Wolfrum (Hrsg.), MPEPIL, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e819?prd=MPIL#law-9780199231690-e819-div1-3 (Rz. 21).

29 Siehe hierzu im Einzelnen das Gutachten von WD 3 zum gleichen Auftrag.

ergeben. Das Bundesverfassungsgericht hat insoweit unter bestimmen Voraussetzungen grundrechtliche Schutzpflichten gegenüber dem Verhalten ausländischer Staaten anerkannt.[30]

3.3.1. Internationale Menschenrechtsinstrumente

Bereits die von der VN-Generalversammlung 1948 verabschiedete Allgemeine Erklärung der Menschenrechte[31] enthält in Art. 12 eine Garantie zum Schutz der Privatsphäre vor willkürlichen Eingriffen. Der Internationale Pakt für Bürgerliche und Politische Rechte (IPbpR)[32] schützt dieses Recht in Art. 17. Die durch Deutschland und Brasilien initiierte Resolution Nr. 68/167 ergänzt, wie oben dargelegt, diesbezüglich den Schutz des Einzelnen vor Eingriffen in seine Privatsphäre auf digitaler Ebene.[33]

3.3.2. Regionale Menschenrechtsabkommen

Die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK)[34] gewährt den der Hoheitsgewalt der Vertragsstaaten unterstehenden Personen in Art. 8 Abs. 1 EMRK das Recht auf Achtung des Privat- und Familienlebens. Im Bereich des Cyberspace prüft der Europäische Gerichtshof für Menschenrechte (EGMR) regelmäßig nicht nur eine Verletzung von Art. 8 EMRK, sondern auch eine Verletzung des Rechts auf freie Meinungsäußerung gem. Art. 10 EMRK, da die Überwachung der Kommunikation dazu führen kann, dass die Betroffenen von ihrer freien Meinungsäußerung abgehalten werden (*chilling effects*).[35]

Nach Art. 8 Abs. 2 EMRK ist eine geheime Überwachung von Bürgern durch staatliche Behörden jedenfalls nur dann zulässig, wenn sie

> 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.

---

30 BVerfGE 55, 349, 364 ff.; 77, 170, 215; BverfGE 14, 192, 199 f.

31 Allgemeine Erklärung der Menschenrechte, Resolution 217 A (III) der Generalversammlung vom 10. Dezember 1948, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/ger.pdf.

32 Internationaler Pakt für Bürgerliche und Politische Rechet (IPbpR), BGBl. 1973 II 1553, https://www.institut-fuer-menschenrechte.de/fileadmin/user_upload/PDF-Dateien/Pakte_Konventionen/ICCPR/iccpr_de.pdf.

33 Siehe unter 2.2.

34 BMJV, Deutsche Übersetzung der EMRK unter Berücksichtigung des Protokolls Nr. 141, Stand: 1. Juni 2010, https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Themenseiten/EuropaUndInternationaleZusammenarbeit/EuropaeischeKonventionMenschenrechte.pdf?__blob=publicationFile&v=1.

35 Siehe weitergehend, Jaber, Der Schutz der Menschenrechte im Cyberspace durch die EMRK, Völkerrechtsblog, Dezember 2016, https://voelkerrechtsblog.org/der-schutz-der-menschenrechte-im-cyberspace-durch-die-emrk/; Ewer/Thienel, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Skandals, NJW 2014, 30, 32.

Der EGMR hat das Recht auf Privatsphäre in zahlreichen Entscheidungen konkretisiert.[36]

Der Schutz der in der EMRK garantierten Rechte gilt gemäß Art. 1 EMRK für alle der Hoheitsgewalt der Vertragsparteien unterstehenden Personen. Ein Staat ist damit grundsätzlich nur auf seinem eigenen Staatsgebiet an die EMRK gebunden. Unter bestimmten Voraussetzungen wirkt die EMRK bei Handlungen eines Staates außerhalb seines eigenen Staatsgebietes aber auch extraterritorial, soweit die jeweiligen Personen der Hoheitsgewalt des Staates unterstehen. Eine derartige extraterritoriale Wirkung wird beispielsweise bei Handlungen des diplomatischen und konsularischen Personals auf fremdem Staatsgebiet angenommen, wenn diese Autorität und Kontrolle über andere ausüben.[37]

Für Mitgliedstaaten der Europäischen Union gilt bei der Durchführung des Rechts der Union[38] die Charta der Grundrechte der Europäischen Union (Grundrechte-Charta).[39] Gemäß Art. 8 Abs. 1 der Grundrechte-Charta hat jede Person das „Recht auf Schutz der sie betreffenden personenbezogenen Daten". Gemäß Abs. 2 dürfen diese Daten nur

> nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

Für die Verarbeitung von personenbezogener Daten durch Behörden der Mitgliedstaaten der Europäischen Union gilt im Unionsgebiet seit dem 25. Mai 2018 zudem die Datenschutz-Grundverordnung (DSGVO)[40]. Die Datenschutz-Grundverordnung hat das europäische Datenschutzrecht modernisiert und zielt insbesondere darauf ab, das Grundrecht auf Schutz der personenbezogenen Daten aus Artikel 8 der Europäischen Grundrechtecharta zu stärken.

Die Datenschutz-Grundverordnung gilt allerdings nur in dem durch Art. 2 der Verordnung festgelegten Anwendungsbereich: Gemäß Art. 2 Abs. 2 lit. a der Verordnung beschränkt sich dieser auf „den Anwendungsbereich des Unionsrechts". Die praktisch bedeutsamste Ausnahme diesbezüglich ergibt sich aus der in Art. 4 Abs. 2 S. 2 EUV vorgesehenen alleinigen Verantwortung der Mit-

---

36 Siehe statt vieler EGMR, *Klass and others ./. Germany*, Urteil vom 6. September 1978, Nr. 5029/71; *Weber and Saravia ./. Germany*, Entscheidung vom 29. Juni 2006, Nr. 54934/00.

37 EGMR, Urteil vom 07.07.2011, *Al-Skeini ./. UK*, Nr. 55721/07, Rn. 133-135; Grabenwarter/Pabel, Europäische Menschenrechtskonvention, 6. Auflage, 2016, § 17 Rn. 16. Vgl. oben Wenzel, a.a.O. (F. 28).

38 Siehe Art. 51 Abs. 1 S. 1 der Europäischen Grundrechte-Charta.

39 Charta der Grundrechte der Europäischen Union, ABl. Der Europäischen Gemeinschaften C 364/01 vom 18. Dezember 2000, https://www.europarl.europa.eu/charter/pdf/text_de.pdf.

40 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, Datenschutz-Grundverordnung (DSGVO), https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE.

gliedstaaten für ihre nationale Sicherheit, für die das Unionsrecht keine Anwendung findet. Insbesondere für die Tätigkeit der Nachrichtendienste der Mitgliedstaaten ist die Verordnung daher nicht anwendbar.[41]

Gemäß Art. 2 Abs. 2 lit. d der Verordnung findet diese auch keine Anwendung auf die Verarbeitung personenbezogener Daten „durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit." Nach der Systematik des deutschen Rechts umfasst dieser Ausnahmetatbestand sowohl die repressive Verfolgung von Straftaten oder Ordnungswidrigkeiten durch Strafverfolgungsbehörden, Gerichte und Ordnungsbehörden als auch die die präventive Verhinderung oder Verhütung von Straftaten durch die Polizei.[42]

Eine Verarbeitung personenbezogener Daten ist gemäß Art. 6 der Verordnung nur mit Einwilligung der betroffenen Person oder unter den weiteren in Artikel 6 genannten Voraussetzungen zulässig, wie beispielsweise dann, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt (Art. 6 Abs. 1 lit. e).

4. Rechtliche Bewertung der Nutzung von sog. IMSI-Catchern durch ausländische Geheimdienste

Vor dem Hintergrund der Fragestellung des Auftraggebers ist ferner die Nutzung von sog. IMSI-Catchern durch ausländische Geheimdienste zu erörtern. „IMSI-Catcher" sind Geräte, mit denen sich die auf der Mobilfunkkarte eines Mobiltelefons gespeicherte Mobilfunkidentität („International Mobile Subscriber Identity" - IMSI) auslesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle eingrenzen lässt.[43] IMSI-Catcher werden hauptsächlich von Strafverfolgungsbehörden und Nachrichtendiensten zur Bestimmung des Aufenthaltsortes einer Person oder zum Erstellen eines Bewegungsprofils genutzt.[44] Soweit IMSI-Catcher von ausländischen Geheimdiensten zu Spionagezwecken eingesetzt werden, muss sich dieser Einsatz im dargelegten völkerrechtlichen Rahmen halten. Werden Geheimdienste von Botschaften aus tätig und setzen sie dabei IMSI-Catcher in einer Art und Weise ein, die gegen deutsche Gesetze verstößt, handeln sie entgegen ihrer Verpflichtungen aus dem Wiener Übereinkommen über diplomatische Beziehungen. Außerdem kommt ein Verstoß gegen menschenrechtliche Verpflichtungen, insbesondere gegen das Recht auf Schutz der Privatsphäre, in Betracht. Erfolgt die geheimdienstliche Tätigkeit

41 Bäcker, in: Wolff/Brink, Beck'scher Online-Kommentar, Datenschutzrecht, Stand. 1. Mai 2019, Art. 2 Rn. 9a.

42 *Ibid.*, Rn. 26.

43 Mallmann, im Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 9 BVerfSchG, Rn 36.

44 Vgl. „Grenzüberschreitende technische Ortung von Personen zur Gefahrenabwehr", WD 3 – 3000- 112/18, 17. April 2018, https://www.bundestag.de/resource/blob/560932/89b883489e411f91a0d3f04119768ecd/WD-3-112-18-pdf-data.pdf.

von einem Mitgliedstaat der Europäischen Union, ist dabei insbesondere die Europäische Grundrechte-Charta zu beachten.

***