die „ultima ratio“ des § 18 Abs. 5 Satz 2 KrWG zurückgreifen, wenn im Vergleich zu einer Untersagungsverfügung mildere Maßnahmen gem. § 18 Abs. 5 Satz 1 KrWG (mangels gleicher Wirksamkeit) ausscheiden. Dies habe die Behörde stets vorab zu prüfen (zweistufige Prüfung)[325]; insoweit handele es sich um eine Ermessensentscheidung (§ 40 LVwVfG, § 114 Satz 1 VwGO)[326].

Insgesamt kristallisiert sich auf der Basis der bislang vorliegenden Rspr. zu den Zulässigkeitsvoraussetzungen gewerblicher Sammlungen, die häufig im Verfahren des vorläufigen Rechtsschutzes ergangen ist, insbesondere der Urteile bzw. Beschlüsse des *VG Ansbach*, *VG Würzburg* sowie der *OVG Hamburg*, *Koblenz* und des *VGH Mannheim*, eine richtungweisende und überzeugende (restriktive) Linie für die Auslegung der §§ 17 f. KrW-/AbfG heraus[327]. Unter Hinweis auf die behördliche Nachweispflicht stellen diese Verwaltungsgerichte zu Recht hohe Anforderungen an die Untersagung einer gewerblichen Sammlung (Art. 12 Abs. 1 GG, Art. 34 ff. AEUV)[328] und gehen in der Tendenz davon aus, dass unwesentliche gewerbliche Sammlungen Privater geduldet werden müssen. Eine vollständige bzw. abschließende Klärung der zahlreichen Auslegungsstreitigkeiten, die sich um die §§ 17 f. KrWG ranken, ist bislang freilich vielfach noch keineswegs eingetreten; dies gilt insbesondere für § 17 Abs. 3 KrWG[329]. Insoweit wird es gewiss zu zahlreichen weiteren Rechtsstreitigkeiten kommen und bleibt die teilweise noch ausstehende Rspr. der *OVG* in den Hauptsacheverfahren sowie im Übrigen vor allem die Rspr. des *BVerwG* und des *EuGH* abzuwarten. Höchstrichterliche Klärung erweist sich in vielen Punkten als unabdingbar, werfen die §§ 17 f. KrWG doch, wie gezeigt, zahlreiche und erhebliche Streitfragen auf, zu deren wissenschaftlicher Klärung die häufig interessengeleitete abfallrechtliche Literatur leider nicht immer beiträgt.

325 *VG Ansbach* (Fn. 298); *VG Düsseldorf*, 18. 12. 2012 – 17 L 1901/12; *Dieckmann/Scherenberg/Zeuschner* AbfallR 2013, 111, 115.

326 *VG Ansbach*, ebd.

327 So auch mit Blick auf § 18 Abs. 5 Satz 2 *Alt. 2* KrWG *Dieckmann/Scherenberg/Zeuschner* AbfallR 2013, 111, 117 ff., 121. Demgegenüber konnte sich die insoweit von einer eher niedrigen Gefährdungsschwelle ausgehende Gegenposition (Fn. 320) bislang – mit Recht – nicht durchsetzen, da sie die kommunalen Interessen unter Vernachlässigung der Gebote zur unions- und verfassungskonformen Auslegung überbewertet. Mit Blick auf § 18 Abs. 5 Satz 2 *Alt. 1* KrWG (Unzuverlässigkeit) dezidiert für eine restriktive Auslegung *OVG Münster* (Fn. 303): „nur bei einem systematischen und massiven Fehlverhalten“.

328 *Klages* AbfallR 2013, 90, 91; vgl. auch *Dieckmann/Scherenberg/Zeuschner* AbfallR 2013, 111, 118.

329 Aber daneben etwa auch für die Vertrauensschutzregelung des § 18 Abs. 7 KrWG und deren Anwendbarkeit auf die gebundene Untersagungsverfügung nach § 18 Abs. 5 Satz 2 KrW. Vgl. verneinend *VG Köln* (Fn. 312) sowie zumindest zweifelnd *OVG Lüneburg* (Fn. 303); bejahend dagegen mit Recht *VG Würzburg* (Fn. 303); wohl auch *VGH München*, 2. 5. 2013 – 20 AS 13 771; offen lassend *VG Ansbach*, 16. 1. 2013 – AN K 12 00 358 = ZUR 2013, 239, m. w. N. Ferner für den Begriff des „Sammlers *VGH Mannheim*, 21. 10. 2013 – 10 S 1201/13 = GewArch 2014, 29; von Abfällen“ (§ 3 Abs. 10 KrWG – Personengesellschaften nicht erfasst): *VGH Mannheim*, 21. 10. 2013 – 10 S 1201/13 = GewArch 2014, 29; *VGH München*, 26. 9. 2013 – 20 BV 13 428 = ZUR 2014, 240; krit. *Oexle/de Diego/Lammers* ZUR 2014, 242; vgl. auch *Petersen/Hermanns* AbfallR 2014, 62.

Kurzbeitrag

Der Begriff der „Hoheitsgewalt“ in Zeiten der Überwachung des Internet- und Telekommunikationsverkehrs durch ausländische Nachrichtendienste

In der Diskussion über die massenhafte anlasslose Überwachung des deutschen Internet- und Telekommunikationsverkehrs durch US-amerikanische und britische Nachrichtendienste wird regelmäßig geltend gemacht, dass diese Überwachungsmaßnahmen gegen völkerrechtliche Normen und insbesondere die Europäische Menschenrechtskonvention (EMRK)[1] und den Internationalen Pakt über bürgerliche und politische Rechte (IPBPR)[2] verstoßen. So haben die Enthüllungen *Edward Snowdens* bereits zu einem derzeit anhängigen Verfahren gegen das Vereinigte Königreich vor dem *EGMR* geführt.[3] Ohne Zweifel handelt es sich bei den Überwachungsmaßnahmen um einen Eingriff in das in Art. 8 EMRK bzw. Art. 17 IPBPR verbürgte Recht auf Achtung des Privatlebens.[4] Meist übersehen oder lediglich beiläufig behandelt wird in der Diskussion dagegen die Frage, ob die beiden Menschenrechtsverträge auf die Überwachungsmaßnahmen der ausländischen Geheimdienste überhaupt anwendbar sind.[5] Dies soll im Folgenden kurz beleuchtet werden.

I. Das Erfordernis der „Hoheitsgewalt“ für den Menschenrechtsschutz

Nach Art. 1 EMRK sichern die Hohen Vertragsparteien „allen ihrer Hoheitsgewalt unterstehenden Personen“ die in der Konvention niedergelegten Rechte und Freiheiten zu. Art. 2 Abs. 1 IPBPR verpflichtet jeden Vertragsstaat „die in diesem Pakt anerkannten Rechte zu achten und sie allen in seinem Gebiet befindlichen und seiner Herrschaftsgewalt unterstehenden Personen […] zu gewährleisten.“ Die Begriffe „Herrschaftsgewalt“ und „Hoheitsgewalt“ sind lediglich zwei unterschiedliche deutsche Übersetzungen des Wortes „jurisdiction“ im authentischen englischen Vertragstext. Im Folgenden wird einheitlich von „Hoheitsgewalt“ gesprochen. Bei dem Erfordernis, dass eine Person der Hoheitsgewalt des Staates untersteht, handelt es sich um ein sogenanntes

1 [Europäische] Konvention zum Schutz der Menschenrechte und Grundfreiheiten v. 4. 11. 1950, BGBl. 2010 II S. 1198.

2 Internationaler Pakt über bürgerliche und politische Rechte v. 19. 12. 1966, BGBl. 1973 II S. 1534.

3 Siehe *Big Brother Watch and Others v. United Kingdom*, No. 58 170/13, Beschwerde v. 4. 9. 2013. Entscheidungen ohne Gerichtsangabe sind solche des *EGMR*. Alle Entscheidungen finden sich auf der Webseite des Gerichts unter http://hudoc.echr.coe.int/.

4 Vgl. *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, 5. Aufl. 2012, Rn. 10, 27; *Nowak*, U.N. Covenant on Civil and Political Rights: CCPR Commentary, 2. Aufl. 2005, Art. 17, Rn. 48; *Esser*, in: *Löwe-Rosenberg*, StPO, Bd. 11: EMRK; IPBPR, 26. Aufl. 2012, Art. 8 EMRK (Art. 17, 23, 24 IPBPR), Rn. 85.

5 Vgl. z. B. *Schmahl* JZ 2014, 220 (227); *Ewer/Thienel* NJW 2014, 30 (32); *Kotzur* ZRP 2013, 216; *Deiseroth* ZRP 2013, 194 (197).

Juristenzeitung 69, 783–787 DOI: 10.1628/002268814X14037757065202
ISSN 0022-6882

„Schwellenkriterium" („threshold criterion"),[6] das heißt eine „notwendige Voraussetzung" für die Anwendbarkeit der Verträge auf einen bestimmten Sachverhalt.[7] Voraussetzung für die Anwendbarkeit der EMRK und des IPBPR auf die Überwachung des Internet- und Telekommunikationsverkehrs durch ausländische Nachrichtendienste ist somit, dass die von den Maßnahmen betroffenen Personen der Hoheitsgewalt des überwachenden Staates unterstehen. In der Literatur wird dies zum Teil generell für alle Überwachungsmaßnahmen bejaht bzw. eine diesbezügliche Annahme de lege ferenda gefordert.[8] Hier ist jedoch zu unterscheiden, ob die Maßnahmen, wie zum Beispiel das Abhören des Mobiltelefons der Kanzlerin durch die US-amerikanische National Security Agency (NSA), im Gebiet eines anderen Staates vorgenommen werden oder ob diese, wie zum Beispiel das „Anzapfen" von Unterseedatenkabeln im Bereich des britischen Küstenmeers durch das britische Government Communications Headquarters (QCHQ), im Gebiet des die Überwachung vornehmenden Staates ergriffen werden.

II. Hoheitsgewalt bei exterritorialen Überwachungsmaßnahmen

Die Hoheitsgewalt der Staaten ist in erster Linie territorial, das heißt räumlich auf ihr Staatsgebiet begrenzt. Maßnahmen, die außerhalb des Staatsgebiets vorgenommen werden oder dort Wirkungen erzeugen („exterritoriale Maßnahmen"), stellen nur in Ausnahmesituationen eine Ausübung von Hoheitsgewalt dar.[9] Ob ausnahmsweise außergewöhnliche Umstände für die Annahme der Ausübung exterritorialer Hoheitsgewalt vorliegen, ist in jedem Einzelfall auf der Grundlage der Tatsachen des Falls zu beurteilen. Voraussetzung für die exterritoriale Ausübung von Hoheitsgewalt ist, dass sich die von der Maßnahme betroffene Person entweder in einem Gebiet aufhält, über das der Staat die wirksame Kontrolle ausübt („effective control over an area"), wie im Falle der militärischen Besetzung fremden Staatsgebiets oder der Herrschaft über eine von ihm abhängige untergeordnete fremde örtliche Verwaltung,[10] oder dass sich die Person in der physischen Gewalt und Kontrolle des Staates befindet („State agent authority and control"), wie im Falle der gewaltsamen Ingewahrsamnahme oder Inhaftierung einer Person im Ausland durch Amtspersonen des Staates.[11]

Die exterritoriale Ausübung von Hoheitsgewalt wird durch das Völkerrecht geregelt und begrenzt.[12] Der Begriff der „Hoheitsgewalt" in den Menschenrechtsverträgen ist im Einklang mit den allgemeinen Regeln des Völkerrechts zu bestimmen.[13] In allen Fällen, in denen eine solche Hoheitsgewaltausübung bejaht wurde, mit Ausnahme der unmittelbaren physischen Gewaltausübung durch Amtsträger,[14] hatte die Ausübung der exterritorialen Hoheitsgewalt eine völkerrechtliche Rechtsgrundlage in der Zustimmung, Einladung oder Duldung durch den Territorialstaat oder im Besatzungsrecht.[15] Dabei übte der betreffende Staat alle bzw. einzelne öffentliche Befugnisse („public powers") der vollziehenden oder rechtsprechenden Gewalt, die normalerweise vom Territorialstaat ausgeübt werden, in Übereinstimmung mit dem Völkergewohnheitsrecht, einem Vertrag oder einer anderweitig erteilten Zustimmung des Territorialstaates aus.[16] Bei den exterritorialen Überwachungsmaßnahmen ausländischer Nachrichtendienste in Deutschland wird es regelmäßig an solch einer Rechtsgrundlage fehlen.

Bei der Überwachung des Internet- und Telekommunikationsverkehrs von Personen im Bundesgebiet durch ausländische Nachrichtendienste üben diese – wenn überhaupt – nur *„virtuelle* Kontrolle" über die Daten im Cyberspace, nicht aber wirksame *„physische* Gewalt und Kontrolle" über die Dateninhaber in Deutschland aus. Sowohl die EMRK als auch der IPBPR stellen jedoch auf Kontrolle über „Personen" ab. Fraglich ist auch bereits, ob eine Erfassung von Verbindungsdaten Kontrolle im Sinne einer Einflussnahmemöglichkeit auf das Verhalten einer Person begründen kann. Eine rein „virtuelle Kontrolle" ist vor dem Hintergrund der Rechtsprechung des *EGMR* nicht ausreichend.[17] So hat der Gerichtshof die Ausübung von Hoheitsgewalt über eine Person bei bloßer „Kontrolle des Luftraums" abgelehnt.[18] Auch die Vertragsstaaten der EMRK haben sich gegen eine extensive Ausdehnung des Erfordernisses der Hoheitsgewaltausübung ausgesprochen.[19] So hat die Bundesregierung im Fall „Weber und Saravia" geltend gemacht, dass eine Person in Argentinien, deren Telekommunikationsverkehr vom Bundesnachrichtendienst überwacht wurde, nicht der Hoheitsgewalt der Bundesrepublik Deutschland unterstand.[20]

Der *EGMR* hat insbesondere der Bestimmung der Hoheitsgewaltausübung ausgehend von der Rechtsverletzung (sog. „cause-and-effect" notion) eine eindeutige Absage erteilt. In seiner Banković-Entscheidung hat der Gerichtshof ausgeführt:

---

6 *Al-Skeini and Others v. United Kingdom* (Grand Chamber [GC]) No. 55721/07, Judgment, 7.7.2011, § 130; *Djokaba Lambi Longa v. Netherlands*, No. 33917/12, Decision, 9.10.2012, § 61.

7 *Catan and Others v. Moldova and Russia* (GC) Nos. 43370/04, 18454/06, 8252/05, Judgment, 19.10.2012, § 103; *Ilaşcu and Others v. Moldova and Russia* (GC), No. 48787/99, Judgment, 8.7.2004, § 311.

8 Siehe z.B. *Milanovic*, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, S. 8, 48, 61, http://ssrn.com/abstract=2418485; *Nyst*, Interference-Based Jurisdiction Over Violations of the Right to Privacy, EJIL:Talk!, 21.11.2013., http://www.ejiltalk.org/.

9 *Al-Skeini* (Fn. 6), § 131; *Banković and Others v. Belgium and Others* (GC), No. 52207/99, Decision, 12.12.2001, §§ 59, 61, 67, 71; *Catan* (Fn. 7), § 104; *Chagos Islanders v. United Kingdom*, No. 35622/04, Decision, 11/12/2012, §§ 70, 71.

10 *Loizidou v. Turkey* (GC), No. 15318/89, Preliminary Objections, 23.3.1995, § 62; *Cyprus v. Turkey* (GC), No. 25781/94, 10.5.2001, § 76; *Banković* (Fn. 9), § 70; *Al-Skeini* (Fn. 6), §§ 138–139.

11 Siehe *Al-Skeini* (Fn. 6), §§ 133–137; *Chagos Islanders* (Fn. 9), § 70; und Human Rights Committee, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add.13, 26.5.2004, S. 4, § 10.

12 *Banković* (Fn. 9), §§ 59, 60; *Medvedyev and Others v. France* (GC), No. 3394/03, Judgment, 29.3.2010, § 65.

13 Siehe z.B. *Ilaşcu* (Fn. 7), § 312; *Ben El Mahi and Others v. Denmark,* Application No. 5853/07, Decision, 11.12.2006.

14 Siehe z.B. *Andreou v. Turkey*, No. 45653/99, Decision, 3.6.2008 (Schuss über die Grenze); UN Human Rights Committee, *Lopez-Burgos v. Uruguay*, Communication No. R.12/52, UN Doc. Supp. No. 40 (A/36/40) at 176 (1981), §§ 12.2–12.3 (Entführung).

15 Vgl. *Al-Skeini* (Fn. 6), §§ 134–136, 138, 139; *Bankovi* (Fn. 9), § 73; *Gentilhomme and Others v. France*, Nos. 48205/99, 48207/99, 48209/99, Judgment, 14.5.2002. In den Fällen der Ausübung von Hoheitsgewalt über Schiffe auf Hoher See hatte diese ihre Grundlage in der Zustimmung des Flaggenstaats; siehe z.B. *Medvedyev* (Fn. 12), § 10; *Rigopoulos v. Spain*, No. 37388/97, Decision, 12.1.1999.

16 Siehe *Al-Skeini* (Fn. 6), § 135.

17 Für „virtuelle Kontrolle" aber z.B. *Peters*, Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part II, EJIL: Talk!, 4.11.2013, http://www.ejiltalk.org/; *Margulies* Fordham Law Review 82 (2014), 2137 (2150–2152). Wie hier *Paust*, Can You Hear Me Now?: Private Communication, National Security, and the Human Rights Disconnect, S. 17, Fn. 35, http://ssrn.com/abstract=2451534.

18 Vgl. *Banković* (Fn. 9), §§ 44, 52, 76.

19 Siehe zuletzt den Vortrag der Niederlande und des Vereinigten Königreichs am 19.2.2014 im Fall *Jaloud v. Netherlands* (GC), No. 47708/08, Webcast der Verhandlung auf http://www.echr.coe.int/.

20 *Weber and Saravia v. Germany*, Application No. 54934//00, Decision, 29.6.2006, § 66. Die Frage wurde vom Gerichtshof nicht entschieden.

„[T]he applicants' notion of jurisdiction equates the determination of whether an individual falls within the jurisdiction of a Contracting State with the question of whether that person can be considered to be a victim of a violation of rights guaranteed by the Convention. These are separate and distinct admissibility conditions, each of which has to be satisfied in the afore-mentioned order, before an individual can invoke the Convention provisions against a Contracting State."[21]

Eine Beeinträchtigung des Rechts auf Leben durch Luftangriffe auf einen anderen Staat im Rahmen eines bewaffneten Konflikts reichte danach für die Begründung exterritorialer Hoheitsgewalt nicht aus. Wenn allein aus der Tatsache der Rechtsverletzung auf die Ausübung von Hoheitsgewalt über eine Person geschlossen werden könnte, könnten potentiell alle Personen weltweit der Hoheitsgewalt der Vertragsstaaten unterstehen. Dies war jedoch niemals intendiert. In diesem Fall wäre das Erfordernis, dass die betroffene Person der Hoheitsgewalt des Staates untersteht, sinnlos und überflüssig. Es käme ihm kein eigenständiger (einschränkender) Gehalt zu. Weiterhin würde die betroffene Person einzig für die spezifische Verletzungshandlung der Hoheitsgewalt des Staates unterstehen. Die Menschenrechtsverträge gehen aber grundsätzlich davon aus, dass die betroffenen Personen der Hoheitsgewalt generell unterstehen.[22]

Die exterritoriale Überwachung des Internet- und Telekommunikationsverkehrs durch ausländische Nachrichtendienste wird danach nicht vom Geltungsbereich der einschlägigen Menschenrechtsverträge erfasst. Eine lediglich inhaltliche Ausdehnung des im IPBPR gewährleisteten Rechts auf Achtung der Privatsphäre auf den Online-Bereich, wie dies in der von Brasilien und Deutschland initiierten Resolution der VN-Generalversammlung Nr. 68/167 v. 18. 12. 2013 angestrebt wird, ist nicht ausreichend, um den begrenzten räumlichen Geltungsbereich des Vertrages zu erweitern. Dass sich aus der Resolution keinerlei (neue) rechtliche Schranken für die exterritoriale Überwachung des Internet- und Telekommunikationsverkehrs ergeben, zeigt sich bereits daran, dass diese im Konsensverfahren, das heißt ohne förmliche Abstimmung, angenommen wurde, und sich weder die USA noch andere in der Auslandsspionage aktive Staaten gezwungen sahen, eine formelle Abstimmung über die Resolution herbeizuführen und gegen diese zu stimmen.[23] Dies ist wenig verwunderlich, da die USA darauf hingewirkt hatten, dass in der endgültigen Fassung der Resolution jeder Hinweis darauf, dass die exterritoriale Überwachung des Telekommunikationsverkehrs das Recht auf Achtung der Privatsphäre verletzt, entfernt wurde. Hatte es im deutsch-brasilianischen Entwurf noch geheißen, dass die Generalversammlung tief besorgt sei „über die *Verletzungen und die Verstöße* gegen die Menschenrechte, die sich aus der […] der exterritorialen Überwachung von Kommunikation […] ergeben können",[24] so heißt es in der Endfassung nur noch, dass die Generalversammlung tief besorgt sei, „über die *nachteiligen Auswirkungen*, die das […] extraterritoriale […] Überwachen […] von Kommunikation […] auf die Ausübung und den Genuss der Menschenrechte haben" kann.[25] Diese Änderung war für die USA notwendige Zustimmungsvoraussetzung, da ihrer Meinung nach die Verpflichtungen aus dem IPBPR zum Schutz der Privatsphäre auf Ausländer außerhalb des US-Staatsgebietes keine Anwendung finden und deshalb auch nicht „verletzt" werden können.[26]

III. Hoheitsgewalt bei intra-territorialen Überwachungsmaßnahmen

Im Völkerrecht besteht eine Vermutung dafür, dass der Staat normalerweise in seinem gesamten Staatsgebiet Hoheitsgewalt ausübt.[27] Soweit Maßnahmen zur Überwachung des ausländischen Datenverkehrs innerhalb des eigenen Staatsgebiets vorgenommen werden (zum Beispiel durch das „Anzapfen" von Datenverbindungen, die durch das Hoheitsgebiet des Staates verlaufen; durch Verfügungen gegen im Staatsgebiet ansässige Internetserviceprovider auf Herausgabe von Datenmaterial, durch die Vorratsdatenspeicherung auf Computern innerhalb des Staatsgebiets oder durch die lokale Auswertung von Daten durch die Nachrichtendienste) wird unzweifelhaft Hoheitsgewalt durch die Nachrichtendienste innerhalb des Gebiets ihres Staates ausgeübt. Bei der Frage der räumlichen Geltung der Menschenrechtsverträge geht es jedoch nicht um die Ausübung von Hoheitsgewalt an sich, sondern darum, dass die von den Überwachungsmaßnahmen betroffenen Personen der Hoheitsgewalt des Staates unterstehen. Daran wird es jedoch regelmäßig fehlen, wenn sich die von der Überwachung betroffenen Personen außerhalb des Gebiets des überwachenden Staates aufhalten.[28] Abzustellen ist nicht auf den Ort der Verletzungshandlung, sondern auf den Aufenthaltsort der von der Verletzung betroffenen Person. So übt die NSA durch die Speicherung der Telefonate der Kanzlerin auf Computern in den Vereinigten Staaten US-amerikanische Hoheitsgewalt aus, die Kanzlerin untersteht damit aber noch nicht der Hoheitsgewalt der Vereinigten Staaten (solange sie sich außerhalb der USA oder eines von diesen kontrollierten Gebiets aufhält).

Der *EGMR* geht grundsätzlich davon aus, dass nur Personen, die sich physisch im Gebiet eines Staates befinden, dessen Hoheitsgewalt unterstehen.[29] So stellte der Gerichtshof zum Beispiel im Fall „Abdul Wahab Khan" fest, dass ein pakistanischer Staatsbürger in Pakistan auch dann nicht der Hoheitsgewalt des Vereinigten Königreichs untersteht, wenn die britische Regierung nachteilige Entscheidungen gegen diesen trifft.[30] Ausnahmen vom Anwesenheitserfordernis bestehen lediglich für Verletzungen des Rechts auf ein faires Verfahren, soweit das Recht des Staates Rechtsschutzmöglichkeiten auch für nicht gebietsansässige Personen vorsieht[31]

21 *Banković* (Fn. 9), § 75. Siehe auch *Medvedyev* (Fn. 12), § 64; *Cattan* (Fn. 7), § 115.

22 *Banković* (Fn. 9), § 75. Siehe aber auch *Al-Skeini* (Fn. 6), § 137, wonach Konventionsrechte „aufgeteilt und zugeschnitten" (divided and tailored) werden können. Dies bedeutet aber nicht, dass die Rechtsverletzung allein Hoheitsgewalt begründet.

23 Die VN-Generalversammlungsresolution Nr. 68/167 wurde am 18. 12. 2013 ohne Abstimmung angenommen; siehe UN Doc. A/68/PV.70 v. 18. 12. 2013, S. 20. Zur Resolution im Einzelnen siehe *Talmon* BRJ 2014, 6 (10 – 12).

24 Siehe den zehnten Absatz der Erwägungsgründe des deutsch-brasilianischen Resolutionsentwurfs, UN Doc. A/C.3/68/L.45 v. 7. 11. 2013.

25 VN-Generalversammlungsresolution Nr. 68/167, Erwägungsgründe, Abs. 10.

26 Siehe das US-Verhandlungspapier Right to Privacy in the Digital Age – U.S. Redlines, abgedruckt bei *Lynch*, Exclusive: Inside America's Plan to Kill Online Privacy Rights Everywhere, 20. 11. 2013, *http://thecable.foreignpolicy.com/*.

27 *Al-Skeini* (Fn. 6), § 131; *Ilaşcu* (Fn. 7), § 312.

28 A.A. *Nyst*, Interference Based Jurisdiction Over Violations of the Right to Privacy, EJIL: Talk!, 21. 11. 2013, *http://www.ejiltalk.org/*. Wie hier *Paust* (Fn. 17), S. 18, Fn. 36.

29 Vgl. *I.R. and G.T. v. United Kingdom*, No. 14 876/12 63339/12, Decision, 28. 1. 2014, § 52; *Djokaba* (Fn. 6), § 69; *Galic v. Netherlands*, No. 22 617/07, Decision, 9. 6. 2009, § 43.

30 *Abdul Wahab Khan v. United Kingdom*, No. 11 987/11, Decision, 28. 1. 2014, §§ 13, 15, 24, 26.

31 Siehe z. B. *Markovic and Others v. Italy* (GC), No. 1398/03, Judgment, 14. 12. 2006, §§ 52 – 55; *K. v. Italy*, No. 38 805/97, Judgment, 20. 7. 2004, § 21.

und für Eingriffe in das im Territorium des Staates gelegene Eigentum einer Person.[32] So führte der Gerichtshof im Fall „Ben El Mahi" unter Hinweis auf die Entstehungsgeschichte der EMRK aus:

> „[T]he words ‚within their jurisdiction' in Article 1 must be understood to mean that a State's jurisdictional competence is primarily territorial […]. The Court has found clear confirmation of this essentially territorial notion of jurisdiction in the travaux préparatoires, given that the Expert Intergovernmental Committee replaced the words ‚all persons residing within their territories' with a reference to persons ‚within their jurisdiction' with a view to expanding the Convention's application to others who may not reside, in a legal sense, *but who are, nevertheless, on the territory of the Contracting States*."[33]

Voraussetzung für die Anwendbarkeit der EMRK (und ebenso des IPBPR[34]) ist also, dass sich die von der Rechtsverletzung betroffene Person „auf dem Gebiet" des Staates befindet. Der *EGMR* hat deshalb die Beschwerde von zwei marokkanischen Staatsbürgern mit Wohnsitz in Marokko, die eine Verletzung ihrer Religionsfreiheit in Dänemark geltend gemacht hatten, mangels eines „Anknüpfungspunktes für die Hoheitsgewalt" („jurisdictional link") zurückgewiesen.[35] Nicht anders aber stellte sich die Situation dar, wenn ein deutscher Staatsbürger mit Wohnsitz in der Bundesrepublik Deutschland eine Verletzung seines Rechts auf Achtung des Privatlebens durch nachrichtendienstliche Überwachungsmaßnahmen im Vereinigten Königreich geltend machen würde. Einziger Anknüpfungspunkt hier wie dort wäre die Rechtsverletzung durch einen Hoheitsakt im Gebiet einer Vertragspartei. Ebenso wie im Fall exterritorialer Maßnahmen eines Vertragsstaates wäre die so begründete Hoheitsgewalt auf die Verletzungshandlung beschränkt. Das Erfordernis, dass die betroffene Person der Hoheitsgewalt des Staates untersteht, wäre in diesem Falle ohne jeden eigenständigen Inhalt. Anknüpfungspunkt für die Verantwortlichkeit der Vertragsstaaten wäre danach nicht mehr, dass Personen „ihrer Hoheitsgewalt unterstehen", sondern dass Personen von „ihren Hoheitsakten betroffen" werden. Ein Verständnis von Hoheitsgewalt, das lediglich an die Rechtsverletzung anknüpft („cause-and-effect" *notion*), würde im Falle der Weitergabe personenbezogener Daten dazu führen, dass die betroffenen Personen der Hoheitsgewalt jedes Vertragsstaates unterständen, an den die Daten weitergegeben werden.

Eine solch weite Auslegung des Hoheitsgewalterfordernisses hätte zudem zur Folge, dass potentiell mehrere Millionen bzw. Milliarden Menschen Beschwerdeführer sein könnten. Bei nachrichtendienstlichen Überwachungsmaßnahmen müssen Beschwerdeführer im Interesse eines effektiven Rechtsschutzes nicht behaupten, selbst Opfer der Maßnahme geworden zu sein, da ihnen dies infolge des geheimen Charakters der Maßnahme meist nicht bekannt sein dürfte. In einem solchen Fall reicht es aus, dass der Beschwerdeführer geltend macht, allein durch die Existenz des die Überwachungsmaßnahmen ermöglichenden Gesetzes oder die Praxis bestimmter Überwachungsmaßnahmen in seinen Rechten betroffen zu sein.[36] Er kann überprüfen lassen, ob ein Gesetz, das Maßnahmen zur Überwachung des Internet- und Telekommunikationsverkehrs ermöglicht, den Anforderungen an die Einschränkung des Rechts auf Achtung des Privatlebens genügt. Das Gericht ermittelt die Opfereigenschaft des Beschwerdeführers dann unter Berücksichtigung der behaupteten Rechtsverletzung, des geheimen Charakters der in Frage stehenden Maßnahmen und der Verbindung zwischen dem Beschwerdeführer und diesen Maßnahmen.[37] Bei Beschwerden gegen Überwachungsgesetze hat der *EGMR* die Anforderungen an die Betroffenheit des Beschwerdeführers weiter gelockert, wenn es auf nationaler Ebene keine Möglichkeit gibt, die angebliche Anwendung geheimer Überwachungsmaßnahmen überprüfen zu lassen. In einem solchen Fall soll eine größere Notwendigkeit für eine Überprüfung durch den Gerichtshof bestehen, auch wenn das tatsächliche Risiko der Überwachung gering ist.[38] Ginge man bei Überwachungsgesetzen mit exterritorialer Wirkung davon aus, dass auch Personen, die sich außerhalb des Gebiets des überwachenden Staates befinden, dessen Hoheitsgewalt unterstehen,[39] wären aufgrund der bei geheimen Überwachungsmaßnahmen geringeren Anforderungen an die Opfereigenschaft alle von einem solchen Überwachungsgesetz betroffenen Personen beschwerdeberechtigt. Auch diese praktische Konsequenz spricht gegen eine Annahme der Hoheitsgewaltausübung über Personen außerhalb des Staatsgebietes.

Das Ergebnis, dass der räumliche Geltungsbereich des IPBPR und der EMRK in Bezug auf die Vertragspartei, welche die grenzüberschreitende Überwachung der Internetnutzung und der Telekommunikation vornimmt, nicht eröffnet ist, bedeutet nicht, dass das Recht auf Achtung des Privatlebens für diesen Sachverhalt ohne Bedeutung ist. Sowohl aus Art. 17 IPBPR als auch aus Art. 8 EMRK ergeben sich nicht nur Abwehrrechte des Einzelnen, sondern auch Schutzpflichten der Staaten.[40] Diese Ansicht wird zwar unter anderem von den USA, dem Vereinigten Königreich und Australien im Hinblick auf Art. 17 IPBPR nicht geteilt,[41] die Mehrheit der Staaten, einschließlich der Bundesrepublik Deutschland, und der Menschenrechtsausschuss der Vereinten Nationen gehen dagegen von einer Schutzpflicht aus.[42] Im Falle einer Überwachung von Internetnutzung und Kommunikationsvorgängen von Personen in Deutschland durch ausländische Nachrichtendienste trifft die Bundesrepublik Deutschland damit eine Pflicht, die persönlichen Daten von Personen in

32 Siehe z. B. *Bosphorus Hava Yollari Turizm Ve Ticaret Anonim Sirketi v. Ireland* (GC), No. 45 036/98, Judgment, 30. 6. 2005, § 137.

33 *Ben El Mahi* (Fn. 13) (Hervorhebung durch den Autor). So bereits auch schon ausführlich die Große Kammer in *Banković* (Fn. 9), §§ 19 – 21, 63.

34 Siehe Human Rights Committee (Fn. 11), S. 4, § 10, wonach Voraussetzung für die Anwendbarkeit des IPBPR ist, dass sich die betroffene Person entweder im Staatsgebiet der Vertragspartei befindet oder unter deren Gewalt und wirksamer Kontrolle steht. Siehe auch *McGoldrick*, in: *Coomans/Kaminga* (eds.), Extraterritorial Application of Human Rights Treaties, 2004, S. 41 (58).

35 Ebd. Der Entscheidung im Fall *Ben El Mahi* scheint die Entscheidung im Fall *Liberty* entgegenzustehen, in der der *EGMR* die Verletzung des Rechts auf Achtung des Privatlebens von zwei irischen NGOs mit Sitz in Dublin bejaht hat, deren Telekommunikationsverkehr mit englischen NGOs von den britischen Behörden im Vereinigten Königreich überwacht wurde. Die Frage, ob die irischen NGOs der Hoheitsgewalt des Vereinigten Königreichs unterstehen, war im Verfahren nicht thematisiert worden, wohl auch deshalb nicht, da die ebenfalls Beschwerde einlegenden britischen NGOs unzweifelhaft der britischen Hoheitsgewalt unterstanden; siehe *Liberty and Others v. United Kingdom*, No. 58 243/00, Judgment, 1. 7. 2008.

36 Siehe *Weber and Saravia* (Fn. 20), § 78.

37 Siehe *Klass and Others v. Germany*, No. 5029/71, Judgment, 6. 9. 1978, § 34.

38 Ebd., § 124; *Hadzhiev v. Bulgaria*, No. 22 373/04, Judgment, 23. 10. 2012, § 39.

39 Bejahend mit Einschränkungen *Jankowska-Gilberg*, Extraterritorialität der Menschenrechte, 2008, S. 164.

40 Siehe *Esser*, in: *Löwe/Rosenberg* (Fn. 4), Rn. 24; *Grabenwarter/Pabel* (Fn. 4), § 22, Rn. 50, 51, 54. Siehe jüngst auch *Jalbă v. Romania*, No. 43 912/10, Judgment, 18. 2. 2014, § 27.

41 Siehe *Nowak* (Fn. 4), Art. 17, Rn. 6.

42 Siehe Human Rights Committee, General Comment No. 16: Art. 17 (The right of respect of privacy, family, home and correspondence and protection of honour and reputation), 8. 4. 1988, UN Doc. HRI/GEN/1/Rev.9 (Vol. I), § 9.

Deutschland, das heißt von Personen, die ihrer Hoheitsgewalt unterstehen, zu schützen, wenn diese durch Dritte – Private oder andere Staaten – beeinträchtigt oder bedroht werden. Die Staaten müssen zweckmäßige und angemessene Maßnahmen treffen, um das Recht auf Achtung des Privatlebens zu sichern. Eine Zusammenarbeit deutscher Stellen mit ausländischen Nachrichtendiensten bei der massenhaften anlasslosen Datenerfassung bzw. die Einräumung des Zugangs zu deutschen Datennetzen ist mit dieser Schutzpflicht nur schwer zu vereinbaren.[43] Bei der Ausübung der Schutzpflicht kommt den Staaten jedoch ein weiter Ermessensspielraum zu. Bei der Ermessensausübung sind neben dem Recht des Einzelnen auf Achtung des Privatlebens auch nationale Sicherheitsinteressen einzubeziehen.[44] Aus der Schutzpflicht ergibt sich damit nicht zwangsläufig eine Pflicht der Bundesrepublik Deutschland (hier des Generalbundesanwalts), ein Ermittlungs- oder Strafverfahren gegen Mitarbeiter ausländischer Nachrichtendienste einzuleiten. In Frage kommen auch technische Schutzvorkehrungen, gesetzliche und diplomatische Maßnahmen sowie, bei Vorliegen eines Verstoßes gegen das Völkerrecht, Klagen oder Staatenbeschwerden vor internationalen Gerichten (soweit die dafür notwendige Gerichtsbarkeit begründet ist). Die Initiative der Bundesregierung zusammen mit Brasilien, eine Resolution der Generalversammlung der Vereinten Nationen auf den Weg zu bringen, in der das Recht auf Achtung des Privatlebens für das digitale Zeitalter ergänzt und fortgeschrieben wird, kann bereits als Maßnahme im Rahmen der Schutzpflicht gewertet werden.

IV. Fazit

Die derzeitige Praxis der massenhaften anlasslosen Überwachung des deutschen Internet- und Telekommunikationsverkehrs durch ausländische Nachrichtendienste dürfte ohne weiteres den Tatbestand des Eingriffs in das Recht auf Achtung des Privatlebens erfüllen, einen Verstoß gegen die einschlägigen Menschenrechtsverträge stellt sie dagegen mangels des begrenzten räumlichen Geltungsbereichs der Verträge nicht dar.[45]

Das Hoheitsgewalterfordernis ist integraler Bestandteil der Menschenrechtsverträge. Es bestimmt den räumlichen Umfang der positiven Verpflichtungen der Vertragsparteien und als solches den Umfang und die Reichweite des vertraglichen Menschenrechtsschutzes – es setzt dem Menschenrechtsschutz eine räumliche Grenze.[46] Die Verträge sind nicht so konzipiert, dass sie jedes Verhalten der Vertragsparteien weltweit erfassen sollen. Das Hoheitsgewalterfordernis kann nicht einfach ignoriert werden, um eine Schutzlücke zu schließen, auch wenn diese vor dem Hintergrund der massenhaften Datenüberwachung als unerträglich angesehen wird. Bei den Menschenrechtsverträgen handelt es sich zwar um lebendige Dokumente („living instruments"), die nicht rein historisch, sondern im Lichte der heutigen (Lebens-)Verhältnisse auszulegen sind, doch kann, wie der *EGMR* in anderem Zusammenhang ausgeführt hat, eine Vertragsbestimmung vom Gerichtshof „nicht nach Belieben aufgehoben [oder interpretiert] werden, um ein angeblich gewünschtes Ergebnis zu erreichen".[47] Auch im Hinblick auf die praktischen Konsequenzen einer Neuinterpretation des Hoheitsgewalterfordernisses im Sinne einer virtuellen Kontrolle über Daten anstelle der physischen Kontrolle über Personen ist hier vor Forderungen nach kreativer richterlicher Rechtsfortbildung zu warnen.

Professor Dr. **Stefan Talmon**, M.A., LL.M.,
Universität Bonn*

43 Zur deutschen Beteiligung am PAMPART-A Programm der NSA siehe NSA ‚third party' partners tap the Internet backbone in global surveillance program, 19. 6. 2014, *http://www.information.dk/501280*.

44 Vgl. *Grabenwarter/Pabel* (Fn. 4), § 22 Rn. 50; *Meyer-Ladewig*, EMRK Handkommentar, 3. Aufl. 2011, Art. 8 Rn. 3.

45 Ebenso *Paust* (Fn. 17), S. 17.

46 *Banković* (Fn. 9), §§ 65, 80; *Medvedyev* (Fn. 12), § 63. Siehe auch bereits *Soering v. United Kingdom*, No. 14038/88, Judgment, 7. 7. 1989, § 86.

47 Siehe *Chagos Islanders* (Fn. 9), § 74. Zu den Grenzen der Interpretation siehe auch *Quark Fishing Ltd. v. United Kingdom*, No. 15305/06, Decision, 19. 9. 2006.

* Der Verfasser war Sachverständiger für die Rechtslage nach Völker- und Europarecht vor dem NSA-Untersuchungsausschuss des Deutschen Bundestages.

Tagungsbericht

Rechtssicherheit durch Rechtswissenschaft

Tagung in Erlangen vom 20. bis 22. Februar 2014

Rechtssicherheit nicht nur als hehres Ziel der theoretischen Auseinandersetzung und der praktischen Anwendung in der Rechtsprechung, sondern gerade als zu förderndes Objekt einer kritischen Wissenschaft, deren Beitrag hierzu festzustellen und zu klären ist, war der Gegenstand der Tagung „Rechtssicherheit durch Rechtswissenschaft" an der Universität Erlangen vom 20. bis 22. Februar 2014. In dem Versuch, den Begriff der Rechtssicherheit zu fassen, gar von unterschiedlichster Perspektive zu beleuchten, führte die von *Jan Schuhr* (Erlangen) organisierte Tagung der Rechtsphilosophie und Rechtstheorie verschriebene Juristen zusammen.

Den Auftakt machte *Susanne Beck* (Hannover). Sie widmete sich dem Begriff der Rechtssicherheit unter dem Gesichtspunkt der gerichtlichen Entscheidungskompetenz und damit der Berechenbarkeit staatlichen Handelns. Ihre zentrale Frage war, ob die Schimäre der einzig richtigen Entscheidung für die Öffentlichkeit notwendig ist. Sie setzte sich damit auseinander, ob es nicht längst fällig wäre, den aus der Unabhängigkeit des Richters geborenen situations- und eigenmotivgebundenen Vorgang der Entscheidungsfindung offenzulegen. *Beck* schlägt hierbei als Lösungsansatz vor, die der Vagheit der Gesetzestexte geschuldete Unsicherheit in der Vorhersehbarkeit bzw. Erkennbarkeit der richterlichen Entscheidung und mögliche anderweitige Motive nicht in die außerrechtliche Welt zu kommunizieren. Denn auch die Kommunikation der Sicherheit der Entscheidung sei ein der Rechtssicherheit innewohnender Wert, der durch Offenbarung der nicht aus dem Recht stammenden Motive und Prämissen gefährdet wäre.

Ganz grundsätzlich widmete sich *Kyriakos Kotsoglou* (Freiburg) der Frage, was Rechtsdogmatik sein könnte. Die Analyse rechtsdogmatischer Strukturen unter Anwendung wissenschaftstheoretischer Ansätze mit der Betonung der Notwendigkeit eines metatheoretischen Diskurses sei hierbei das Ziel. Die strikte Einordnung der Rechtswissenschaft zwischen Formalismus und Dezisionismus beruhe auf einem „myth of the given" und sei hinfällig. Sie habe eine falsche Orientierung des Wissenschaftsbetriebes zur Folge. *Kotsoglou* verglich die Rechtsdogmatik mit naturwissenschaftlichen Modellen und zeigte hierbei, dass zur Vermeidung eines „myth of the valid" Rechtsdogmatik unverzichtbar ist. Die Existenz objektiver Werte sei ebenso wie die natürlicher Fak-

Juristenzeitung 69, 787–788 DOI: 10.1628/002268814X13959125974888
ISSN 0022-6882