6

PRZEMYSŁAW ROGUSKI

Globale Internetüberwachungsprogramme und der Menschenrechtsschutz

Programy masowej inwigilacji internetowej a międzynarodowa ochrona praw człowieka

Tajne dokumenty amerykańskie opublikowane przez byłego pracownika wywiadu NSA, Edwarda Snowdena, ujawniły masową skalę inwigilacji internetu prowadzoną przez USA, Wielką Brytanię oraz inne państwa. Rodzi to pytanie co do zasadności tych programów, z jednej strony, oraz stosownej ochrony praw człowieka, w tym prawa do prywatności w internecie, z drugiej strony. Celem niniejszego opracowania jest odpowiedź na pytanie, czy i jakie ograniczenia dla kontroli komunikacji elektronicznej prowadzonej za pośrednictwem internetu ustanawiają międzynarodowe instrumenty ochrony praw człowieka, w szczególności Międzynarodowy Pakt Praw Obywatelskich i Politycznych (MPPOiP).

Opracowanie jest podzielone na cztery części. W części pierwszej, wprowadzającej, prezentuje się zasięg inwigilacji internetu w ramach programów UPSTREAM i TEMPORA. Drugą część poświęca się rozważaniom, czy programy masowej inwigilacji podlegają MPPOiP *ratione loci*. Konwencja zobowiązuje państwa do zagwarantowania praw i wolności osobom podlegającym ich jurysdykcji oraz będącym na ich terytorium. Ponieważ inwigilacja w ramach ww. programów ma charakter ekstraterytorialny, a więc przechwytywana jest przede wszystkim komunikacja osób przebywających poza terytorium danego państwa, należy najpierw ustalić, czy osoby, których komunikacja jest kontrolowana, w inny sposób podlegają jurysdykcji inwigilującego państwa. W trzeciej części opracowania omawia się zakres ochrony prawa do prywatności w internecie oraz dopuszczalność ingerencji. Ostatnia części obejmuje podsumowanie i konkluzję.

Программы массового наблюдения в интернете и международная защита прав человека

Секретные документы США, опубликованные бывшим сотрудником разведки АНБ (*National Security Agency*), Едвардом Сноуденом (*Edward Snowden*), показали

масштаб слежения проводимого в Интернете службами США, Великобритании и других стран. Это накладывает вопрос, являются ли данные программы, во-первых, оправданы, а во-вторых, совместимы с защитой прав человека, включая право на неприкосновенность частной жизни в Интернете. Целью этого исследования является ответ на вопрос, существуют ли ограничения в сфере допустимости контроля электронной связи, проводимого посредством Интернета, установленные международными правовыми актами по защите прав человека, в частности Международным пактом о гражданских и политических правах (МПГПП), и если так, то какие.

Исследование состоит из четырех частей. В первой, вводной части, представлена сфера действия программ наблюдения в Интернете – UPSTREAM и TEMPORA. Вторая часть посвящена рассуждениям, распространяется ли на программы массового наблюдения *ratione loci* МПГПП. Конвенция обязывает государство гарантировать права и свободы лицам находящимся в их юрисдикции и пребывающим на их территории. Наблюдение в рамках вышеупомянутых программ имеет экстратериториальный характер, так как они перехватывают прежде всего связь лиц, проживающих за пределами территории данного государства. Поэтому в первую очередь необходимо определить, подлежат ли лица, коммуникация которых контролируется, юрисдикции государства ведущего наблюдение. В третьей части исследования рассматриваются границы защиты права на частную жизнь в Интернете и допустимость вмешательства. Последняя часть представляет собой заключение и выводы.

Globale Internet-Überwachungsprogramme und der internationale Menschenrechtsschutz

Die von Edward Snowden veröffentlichten Unterlagen des amerikanischen Geheimdienstes NSA offenbarten das massive und globale Ausmaß der Internetüberwachung, welche durch die Vereinigten Staaten, das Vereinigte Königreich und andere Staaten unternommen wird. Dies wirft die Frage nach der Rechtmäßigkeit dieser Programme und nach der Wirksamkeit des Schutzes der Menschenrechte, insbesondere des Rechts auf Privatsphäre, auf. Das Ziel dieser Abhandlung ist die Antwort auf die Frage, ob – und falls ja, welche – Beschränkungen für die Kontrolle elektronischer über das Internet geführter Kommunikation die internationalen Menschenrechtsabkommen, insbesondere der Internationale Pakt über bürgerliche und politische Rechte (IPbpR), auferlegen.

Die Abhandlung besteht aus vier Teilen. Im ersten, einführenden Teil wird der Umfang der Internetüberwachung anhand der Programme UPSTREAM und TEMPORA beschrieben. Der zweite Teil ist Überlegungen gewidmet, ob die Menschenrechtspakte hinsichtlich der Massenüberwachungsprogramme *ratione loci* anwendbar sind. Die Konvention verpflichtet die Mitgliedstaaten, die Konventionsrechte allen ihrer Hoheitsgewalt unterstehenden und auf ihrem Gebiet befindlichen

Personen zu gewähren. Da die Überwachung im Rahmen der o.g. Programme extraterritorialen Charakter hat, d.h. vor allem die Kommunikation von Personen, die sich außerhalb des Staatsgebiets des kontrollierenden Staates befinden, überwacht wird, muss zuerst geklärt werden, auf welche Weise diese Personen der Hoheitsgewalt des überwachenden Staates unterliegen. Im dritten Teil des Beitrags wird der Schutzbereich des Rechts auf Privatsphäre im Internet sowie die Zulässigkeit eines Eingriffs besprochen. Der letzte Teil enthält eine Zusammenfassung und Schlussfolgerungen.

I. Einleitung

Das 21. Jahrhundert ist das Jahrhundert der digitalen Revolution. Immer mehr Aspekte des menschlichen Lebens wie Kommunikation oder der Genuss verschiedener Dienstleistungen finden elektronisch und in einer global vernetzten Umgebung statt. E-Mail, soziale Netzwerke und andere Kommunikationstechnologien haben dazu beigetragen, dass immer mehr Aspekte des täglichen Lebens, inklusive eines erheblichen Bereichs der Privat- und sogar Intimsphäre, „ins Netz" verlagert werden. Moderne Informationstechnik hat somit „für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt"[1].

Die Verbreitung moderner Informations- und Kommunikationstechnik hat somit einerseits zu einer Erweiterung der Sphäre persönlicher Freiheit geführt, andererseits aber auch neue Gefahren für diese Freiheit entstehen lassen. Internetgestützte Kommunikationsmethoden und soziale Netzwerke dienen nicht nur zum besseren Informationsaustausch unter Bürgern, sondern auch Gruppen, die die wirtschaftliche Betätigung im Internet gezielt angreifen (Computerkriminalität)[2] oder – wie durch die furchtbaren Terroranschläge in Paris und Brüssel verdeutlicht – das Internet zur Koordination von Angriffen auf Leib und Leben und Verbreitung radikaler Ideologien benutzen. Dies wiederum hat die Staaten dazu veranlasst, Internetaktivitäten stärker zu regulieren und zu kontrollieren, was seinerseits hoheitliche Eingriffe in den computer- und netzgestützten Raum persönlicher Freiheit möglich macht. Die Verlagerung der

---

1 Bundesverfassungsgericht (BVerfG), Urteil vom 27. Februar 2008, Az. 1 BvR 370/07 und 1 BvR 595/07, Rn. 170.

2 Vgl. Polnischer Verfassungsgerichtshof (*Trybunał Konstytucyjny*, hiernach: Poln. VerfGH), Urteil vom 30. Juli 2014, Az. K 23/11, S.51 Rn. 1.6.

Persönlichkeitsentfaltung und Kommunikation ins Netz verstärkt die potentielle Intensität staatlicher Grundrechtsbeschränkungen.

Die Gefahr, die von staatlicher Kontrolle moderner Informationstechnologie für die Grundrechtsausübung ausgeht, wurde auf innerstaatlicher Ebene früh erkannt und von der ordentlichen bzw. Verfassungsgerichtsbarkeit entsprechend thematisiert. In seinen Urteilen zur Online-Durchsuchung[3] und Vorratsdatenspeicherung[4] stellte das Bundesverfassungsgericht (BVerfG) nicht nur die besondere Bedeutung moderner Informationstechnik für die Persönlichkeitsentfaltung fest, sondern setzte den staatlichen Organen klare Grenzen für Eingriffe in Kommunikations- oder Persönlichkeitsgrundrechte im Online-Bereich. Auch der polnische Verfassungsgerichtshof hatte sich mit der Verfassungsmäßigkeit der Überwachungstätigkeit staatlicher Organe zu befassen[5]. In seinem, aus verschiedenen Gründen beachtlichen[6], Urteil vom 30. Juli 2014 stellte der Poln. VerfGH fest, dass der technische Fortschritt und moderne (Kommunikations-) Technologien die Sphäre menschlicher Freiheit erweitern und die mit ihrer Hilfe vorgenommene Freiheitsbetätigung unmittelbar durch die Verfassung geschützt ist[7]. Zudem betonte er, dass im demokratischen Rechtsstaat die Organisation des gesellschaftlichen und öffentlichen Zusammenlebens für den Einzelnen die Möglichkeit bewahren muss, seine Anonymität gegenüber dem Staat und Dritten gleichermaßen zu schützen[8]. Gleichzeitig besteht für die Staatsorgane Kraft Verfassung ein Schutzauftrag gegenüber dieser verfassungsrechtlich garantierten Grundrechtsausübung. Um diese Aufgabe wahrzunehmen, müssen die Kompetenzen und Handlungsmöglichkeiten der Staatsorgane rechtlich und faktisch so ausgestaltet werden, dass ein hinreichender Schutz gewährleistet werden kann[9]. Der Schutzauftrag bezieht sich dabei nicht nur auf das unbefugte Handeln Dritter, sondern auch auf Gefahren, die außerhalb des Staates verortet sind und insbesondere von den Handlungen anderer Staaten herrühren[10].

Mit dem Hinweis, dass der Staat die Kommunikationsfreiheit und die Privatsphäre seiner Bürger auch vor Eingriffen anderer Staaten zu schützen hat,

---

3 BVerfG, Urteil vom 27. Februar 2008, Az. 1 BvR 370/07 und 1 BvR 595/07, BVerfGE 120, 274–350.

4 BVerfG, Urteil vom 02. März 2010, Az. 1 BvR 256/08, BVerfGE 125, 260–385.

5 Poln. VerfGH, Urteil vom 30. Juli 2014, Az. K 23/11.

6 U.a. wegen seiner umfangreichen rechtsvergleichenden Analyse und Untersuchung der Spruchpraxis anderer europäischer Verfassungsgerichte sowie des Europäischen Gerichtshofs für Menschenrechte.

7 Poln. VerfGH, Urteil vom 30. Juli 2014, Az. K 23/11, S. 50ff., Rn. 1.4–1.6.

8 *Ibid.*

9 Poln. VerfGH, Urteil vom 30. Juli 2014, Az. K 23/11, S. 52 Rn. 1.7.

10 Poln. VerfGH, Urteil vom 30. Juli 2014, Az. K 23/11, S. 56 Rn. 1.13.

deutet der VerfGH auf die von Edward Snowden enthüllten Überwachungsprogramme des US-amerikanischen Geheimdienstes *National Security Agency* (*NSA*) und des britischen *General Communications Headquarters* (*GCHQ*) hin. Wie aus den von Snowden ans Licht gebrachten Geheimdokumenten hervorgeht, führten der GCHQ mit TEMPORA[11] und der NSA mit UPSTREAM[12] Programme zur massenweisen Überwachung von internetbasierter Telekommunikation. Beide Geheimdienste errangen Zugang zu Unterseekabeln, über die der gesamte transatlantische Datenaustausch geleitet wird und die somit das technische Rückgrat des Internet darstellen. Der Zugriff auf diese Kabel, welcher teilweise durch Installation von technischen Einrichtungen auf den Kabeln selbst erfolgte[13], ermöglichte es den Geheimdiensten, Metadaten und Inhalte der über diese Kabel laufenden Kommunikation in Echtzeit mitzuverfolgen und so Millionen Gigabytes an Daten für eine spätere Auswertung zu speichern[14].

Der Umfang der durch technischen Fortschritt möglichen Massenüberwachung lenkte die Aufmerksamkeit auf ein bis dahin nur ungenügend behandeltes rechtliches Problem: obschon die nationalen Gesetzgeber und vor allem die Verfassungsgerichte den Zugriff staatlicher Organe auf Daten der eigenen Staatsbürger bzw. sich im Geltungsbereich der Verfassung aufhaltenden Personen beschränken und in verfassungsrechtliche Rahmen setzen konnten, blieb das auswärtige Handeln von Staatsorganen (insbesondere Auslandsgeheimdiensten) im Bereich der Fernmeldeaufklärung und Telekommunikationsüberwachung wegen seines Bezugs zur nationalen Sicherheit entweder geringeren rechtlichen Anforderungen unterworfen, oder aber zumeist weniger streng kontrolliert. Dies mag bei der Überwachung der Kommunikation fremder Staatsorgane seine Begründung haben; hingegen wirft die massenhafte Überwachung privater Kommunikation im Ausland zwei Fragen auf, die Gegenstand der nachfolgenden Untersuchung sein sollen: *erstens*, ob die Überwachung der Kommunikation von Ausländern im Ausland denselben rechtlichen Anforderungen unterworfen ist, wie die Überwachung von Inlandskommunikation und *zweitens*, wie diese Anforderungen im Einzelnen ausgestaltet sind. Prüfungsmaßstab für die

---

[11] D.P. Fidler, *The Snowden Reader*, Bloomington: Indiana University Press, 2015, S. 201f.

[12] *Ibid.*, S. 97.

[13] Vereinte Nationen, Bericht des Sonderbeauftragten Ben Emmerson vom 23 September 2014 (*Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*), A/69/397, Rn. 25.

[14] Für eine zusammenfassende Darstellung der Massenüberwachungsprogramme siehe Europarat, Committee on Legal Affairs and Human Rights, *Report on Mass Surveillance* vom 18. März 2015, Doc. 13734.

Untersuchung soll dabei der Internationale Pakt über bürgerliche und politische Rechte (IPbpR)[15] sein.

II. Anwendbarkeit des Menschenrechtspaktes auf extraterritoriale Überwachungsmaßnahmen

Die Überwachung von Ausländern außerhalb des Staatsgebiets stellt eine extraterritoriale Maßnahme staatlicher Organe dar. Wird die Überwachung, wie etwa im britischen TEMPORA-Programm, über das „Anzapfen" von Unterseekabeln geführt, liegt zudem der Zugriff auf die Telekommunikationsdaten nicht nur außerhalb des eigenen Staatsgebiets[16], sondern insgesamt außerhalb jeglichen Staatsgebiets. Die erste Frage, die es zu untersuchen gilt, lautet daher, ob diese Abhörmaßnahme überhaupt in den Anwendungsbereich des IPbpR fällt und somit an ihm zu messen ist. Art. 29 der Wiener Vetragsrechtskonvention[17] besagt nämlich, dass ein Vertrag jede Vertragspartei hinsichtlich ihres gesamten Hoheitsgebiets, allerdings eben nur des Hoheitsgebiets, bindet. Gemäß Art. 2 I IPbpR verpflichtet sich jeder Vertragsstaat, die in dem Pakt anerkannten Rechte zu achten und sie „allen in seinem Gebiet befindlichen und seiner Herrschaftsgewalt unterstehenden Personen" zu gewährleisten. Im Kontext grenzüberschreitender Überwachungsmaßnahmen wie der oben beschriebenen UPSTREAM- und TEMPORA-Programme wirft diese Klausel die Frage auf, ob im Falle des IPbpR für eine Verpflichtung des Staates beide Voraussetzungen („Gebiet […] und […] Herrschaftsgewalt") kumulativ vorliegen müssen, oder ob die Vertragsstaaten auch bei Handlungen außerhalb ihres Staatsgebiets zur Gewährleistung der Konventionsrechte verpflichtet sind, sofern eine Person ihrer Herrschaftsgewalt untersteht.

Die kumulative Auslegung der Voraussetzungen von Art. 2 I IPbpR wird vor allem von den Vereinigten Staaten von Amerika vertreten. Seit einer mündlichen Stellungnahme des Rechtsberaters der US-Regierung (*Legal Advisor*) *C. Harper* im Jahre 1995[18] vertreten die USA die Position, wonach die Wortlautinterpretation des Art. 2 I eine extraterritoriale Anwendung der Konvention

---

[15] Internationaler Pakt über bürgerliche und politische Rechte vom 19. Dezember 1966, deutsche Fassung abgedruckt in: BGBl. 1973 II S. 1553.

[16] Sofern die Abhörinstallation auf dem Teil des Kabels, welches außerhalb des Küstenmeeres liegt, angebracht wird.

[17] Wiener Übereinkommen über das Recht der Verträge vom 23. Mai 1969, deutsche Fassung abgedruckt in: BGBl. 1985 II S. 927.

[18] UN Menschenrechtsausschuss, U.N. Doc. CCPRIC/SR 1405, Rn. 20.

ausschließt[19]. Die Konjunktion „und" weise bereits semantisch darauf hin, dass sowohl Gebiet, als auch Herrschaftsgewalt vorliegen müssen. Neben der Wortlautauslegung wird zudem auf die *travaux préparatoires* verwiesen. Bei der Diskussion zum Wortlaut des Art. 2 wurde von der damaligen US-Repräsentantin *E. Roosevelt* darauf hingewiesen, dass jene Situationen ausgeschlossen werden sollten, wonach eine Person zwar der Herrschaftsgewalt der Vereinigten Staaten unterstellt sei, aber sich nicht auf deren Territorium befinde, also beispielsweise Personen in unter US-Besatzung stehenden Gebieten wie Teile des damaligen (West-)Deutschlands[20].

In dieser Interpretation des Art. 2 IPbpR sind die USA allerdings weitgehend allein. So hat beispielsweise der Internationale Gerichtshof (IGH) in seinem Mauer-Gutachten[21] und dem Urteil in der Rechtssage *Kongo v. Uganda*[22] festgestellt, dass *jurisdiction* (im Sinne der Herrschaftsgewalt) zwar primär gebietsbezogen sei, jedoch auch außerhalb des eigenen Staatsgebiets ausgeübt werden köhne[23]. Zumindest in den Fällen, in denen ein Staat fremdes Staatsgebiet okkupiert oder effektive Kontrolle darüber ausübt, kann er der Ausdehnung seiner Konventionsverpflichtungen auf diese Gebiete nicht entkommen. Denn den Verfassern der Konvention sei es eben nicht darum gegangen, den Vertragsstaaten die Flucht vor Konventionsverpflichtungen durch Auslandshandlungen zu ermöglichen, sondern lediglich darum, auszuschließen, dass im Ausland lebende Staatsbürger gegenüber ihren Herkunftsstaaten Rechte geltend machen, die unter die Herrschaftsgewalt und Regelungskompetenz des Aufenthaltsstaates fallen[24]. Nach dem IGH gilt dies nicht nur für die Fälle staatlicher Gebietskontrolle, sondern alle Fälle der Ausdehnung staatlicher Herrschaftsgewalt auf Personen im Ausland.

---

[19] Vgl. z.B. U.S. Department of State, *List of Issues to be Taken Up in Connection with the Consideration of the Second and Third Periodic Reports of the United States of America*, Question 4, U.N. Menschenrechtsausschuss (17.07.06), abrufbar unter http://www.state.gov/j/drl/rls/70385.htm [zuletzt abgerufen am: 28.02.2016].

[20] *Compilation of the Comments of Governments on the Draft International Covenant on Human Rights and on the Proposed Additional Articles*, 14, U.N. Doc. E/CN.4/365, Rn. 41.

[21] IGH, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Gutachten vom 9. Juli 2004, ICJ Rep. 2004, S. 136 [hiernach: Mauer-Gutachten].

[22] IGH, *Case Concerning Armed Activities on the Territory of the Congo* (Dem. Rep. Kongo v. Uganda), ICJ Rep. 2005, S. 334 [hiernach: Kongo v. Uganda].

[23] „*The Court would observe that, while the jurisdiction of States is primarily territorial, it may sometimes be exercised outside the national territory*". IGH, *Kongo v. Uganda*, Rn. 109.

[24] IGH, *Mauer-Gutachten*, Rn. 109 unter Verweis auf United Nations, Official records of the General Assembly, Tenth Session, Annexes, Al2929, Part II, Chap. V, para. 4 (1955).

Diese Auslegung teilt auch der UN-Menschenrechtsausschuss in seinen Mitteilungen über die Streitsachen *Lopez Burgos v. Uruguay*[25] und *Montero v. Uruguay*[26]. Im ersten Fall ging es um die Entführung eines uruguayischen Staatsbürgers durch uruguayische Sicherheitskräfte aus Argentinien, während im zweiten Fall einem in Berlin ansässigen uruguayischen Staatsbürger vom uruguayischen Konsulat die Verlängerung seines Reisepasses verweigert wurde. Beiden Fällen ist die extraterritoriale Ausübung der staatlichen Herrschaftsgewalt gemein. Dennoch sah der Menschenrechtsausschuss kein Problem darin, die Ausübung der Herrschaftsgewalt über eine Person, die sich nicht auf dem Staatsgebiet des Herkunftsstaates aufhielt, zur Begründung der Jurisdiktion im Sinne des Art. 2 IPbpR als ausreichend zu erachten. In *Lopez Burgos* stellte er vielmehr klar, dass „Herrschaftsgewalt" im Sinne des 1. Zusatzprotokolls (welches Individualklagen regelt und anders als Art. 2 IPbpR das Staatsgebiet nicht erwähnt) nicht den Ort, an dem die staatliche Handlung vorgenommen wurde, meint, sondern die rechtliche Beziehung zwischen dem Individuum und dem Staat in Bezug auf Konventionsverletzungen, unabhängig vom Ort, an dem sie stattfanden[27]. Eine andere Interpretation des Art. 2 IPbpR (im Sinne der kumulativen Voraussetzung von Staatsgebiet und Herrschaftsgewalt) liefe vielmehr Art. 5 Abs. 1 IPbpR entgegen, wonach keine Bestimmung des Paktes so auszulegen ist, dass sie für den Staat das Recht begründet, Tätigkeiten auszuüben oder Handlungen vorzunehmen, die auf die Abschaffung oder weitgehende Beschränkung von Konventionsrechten hinzielen[28]. Sollte extraterritorial ausgeübte Herrschaftsgewalt aus dem Geltungsbereich der Konvention ausgenommen sein, liefe dies aber auf eine faktische Abschaffung der Konventionsgarantien gegenüber den dieser extraterritorialen Herrschaftsgewalt unterstehenden Personen hinaus. Diese Interpretation bestätigte der Menschenrechtsausschuss zudem in *General Comment Nr. 31*[29].

Diese Interpretation des Paktes hat der Menschenrechtsausschuss auch speziell für Internetüberwachung bestätigt. In seinen abschließenden Bemerkungen zum Vierten Periodischen Bericht der USA[30] und zum Siebten Periodi-

---

[25] Menschenrechtsausschuss, *Sergio Euben Lopez Burgos v. Uruguay*, Communication No. R.12/52, U.N. Doc. Supp. No. 40 (A/36/40) [hiernach: *Lopez Burgos v. Uruguay*].

[26] Menschenrechtsausschuss, *Mabel Pereira Montero v. Uruguay*, Communication No. 106/1981, U.N. Doc. Supp. No. 40 (A/38/40).

[27] Menschenrechtsausschuss, *Lopez Burgos v. Uruguay*, Rn. 12.2.

[28] *Ibid.*, Rn. 12.3.

[29] Menschenrechtsausschuss, *General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant*, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004), Rn. 10.

[30] Menschenrechtsausschuss, *Concluding observations on the fourth periodic report of the United States of America*, CCPR/C/USA/CO/4, Rn. 22.

schen Bericht Großbritanniens[31], brachte der Menschenrechtsausschuss seine Besorgnis über die Überwachungsaktivitäten beider Staaten, u.a. im Rahmen der Programme TEMPORA und UPSTREAM, zum Ausdruck und legte beiden Staaten auf sicherzustellen, dass der Schutz der Konventionsrechte, insbesondere des Rechts auf Schutz der Privatsphäre nach Art. 17 IPbpR, gewährleistet wird „unabhängig von der Nationalität **und vom Aufenthaltsort** [eigene Hervorhebung] der Personen, deren Kommunikation einer direkten Überwachung unterliegt"[32].

Die vom Menschenrechtsausschuss in seinen abschließenden Bemerkungen vertretene Ansicht stellt zwar das Ergebnis der Auslegung von Art. 2 Abs. 1 IPbpR dar, schweigt aber hinsichtlich der dogmatischen Begründung dieses Ergebnisses im Hinblick auf die Überwachung von Internetkommunikation. Im Gegensatz zu den oben geschilderten vom IGH und dem Menschenrechtsausschuss betrachteten Fallgestaltungen, etwa im *Mauer-Gutachten*[33], oder *Lopez Burgos*[34], stellt das Abhören von Unterseekabeln nämlich weder einen Fall der effektiven Kontrolle über fremdes Staatsgebiet, noch der physischen Kontrolle über das Individuum im Sinne einer „*state agent authority and control*"[35] dar[36]. Der Zugriff auf das Kabel erfolgt vielmehr außerhalb jeglichen Staatsgebiets (auf hoher See) und zu keiner Zeit übt der Staat physische Kontrolle über die betroffene Person aus.

Im Schrifttum sind daher verschiedene dogmatische Figuren diskutiert worden. So schlägt beispielsweise *P. Margulies* vor, das Kriterium der effektiven Kontrolle, welches sowohl der territorialen, als auch der personalen Herrschaftsgewalt iSd Art. 2 Abs. 1 IPbpR zugrunde liegt, auf den Cyberraum zu erweitern[37]. Demnach solle effektive Kontrolle im Sinne einer

---

[31] Menschenrechtsausschuss, *Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland*, CCPR/C/GBR/CO/7, Rn. 24.

[32] „*In particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance*". *Ibid.*

[33] IGH, Gutachten vom 9 Juli 2004, ICJ Rep. 2004, S. 136.

[34] Menschenrechtsausschuss, Communication No. R.12/52, U.N. Doc. Supp. No. 40 (A/36/40).

[35] Vgl. Europäischer Gerichtshof für Menschenrechte, Urteil vom 7 Juli 2011, *Al-Skeini and Others v. United Kingdom*, Application no. 55721/07, Rn. 134–137.

[36] Für eine umfangreiche Darstellung der internationalen Rechtsprechung zur extraterritorialen Anwendung von Menschenrechtspakten siehe die Abhandlung von M. Milanovic, *Extraterritorial Application of Human Rights Treaties*, Oxford: Oxford University Press, 2011, S. 118ff. mwN.

[37] P. Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, „Fordham Law Review" 2014, S. 2150–51.

„virtuellen Kontrolle" (*virtual control test*) vorliegen, wenn der Staat ferngesteuert Kontrolle über die Kommunikation einer Person ausüben kann, unabhängig davon wo sich die Person befindet und ob der Staat physische Kontrolle über sie ausübt[38]. Hingegen schlägt der Hohe Kommissar der Vereinten Nationen für Menschenrechte (UNHCHR) einen etwas anderen Weg ein und stellt in seinem Bericht nicht auf die Kontrolle über den Inhalt der Kommunikation, sondern auf die Kontrolle über die technischen Kommunikationseinrichtungen ab: „[...] *digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure*"[39]. Dasselbe solle gelten, wenn der Staat regulatorische Herrschaftsgewalt über einen Dritten, der Zugang zu den Kommunikationsinhalten hat, ausübt[40].

Beiden vorgestellten Lösungsansätzen ist gemein, dass sie die vom Staat ausgeübte Kontrolle orts- und personenunabhängig erklären und somit für das Internet tauglich machen. Jedoch bringt das Formulieren neuer „Tests" bzw. eine von den technischen Gegebenheiten abhängige Betrachtung zu dem Risiko, dass manche speziellen Fallgestaltungen übergangen werden können. Vorzugswürdig ist daher ein Ansatz, der den Anwendungsbereich des Art. 2 IPbpR technikunabhängig herleitet. Nach Ansicht des Autors läge ein solcher Ansatz nicht in der Ausübung effektiver Kontrolle über das Gebiet, die Person oder die Technik, mithilfe derer kommuniziert wird, sondern in der Ausübung effektiver Kontrolle über die konventionsrechtlich vor Eingriff geschützte Tätigkeit bzw. die eigentliche Rechtewahrnehmung (*effective control over the enjoyment of a right*). Eine solche Argumentationsfigur lässt sich aus der bisherigen Rechtsprechung des Menschenrechtsausschusses aber auch des Europäischen Gerichtshofs für Menschenrechte begründen. So war im Fall *Montero* nicht etwa die vom Konsularbeamten ausgeübte physische Kontrolle über die Person, sondern vielmehr die Kontrolle über das von dieser Person geltend gemachte Recht entscheidend[41]. Ebenso sah der EGMR die Anwendbarkeit der Konvention in den Fällen *Loizidou*[42] und *Bosphorus*[43],

---

38 *Ibid.*

39 UNHCHR, Bericht vom 30. Juni 2014, The Right to Privacy in the digital age, A/HRC/27/37, Rn. 34 [Hiernach: UNHCHR Bericht].

40 *Ibid.*

41 Menschenrechtsausschuss, *Mabel Pereira Montero v. Uruguay*, Communication No. 106/1981, U.N. Doc. Supp. No. 40 (A/38/40).

42 EGMR, Urteil vom 23. Februar 1995, *Loizidou v. Turkey*, Az. 40/1993/435/514.

43 EGMR, Urteil vom 30. Juni 2005, *Bosphorus Hava Yollari v. Ireland*, Az. 45036/98.

in denen die Staaten effektive Kontrolle über das Eigentum der Beschwerdeführer ausübte, beide Beschwerdeführer weder Staatsbürger der handelnden Staaten, noch auf deren Territorium präsent waren, unproblematisch als gegeben an. Die hier vertretene Ansicht wird auch von einigen Staaten geteilt. So haben Österreich, Liechtenstein, Slowenien und die Schweiz in einem gemeinsamen Brief an den UN-Menschenrechtskommissar ihre Position wie folgt zusammengefasst: „*In other words, the extraterritoriality of States Parties' human rights obligations is not categorical. A State Party is subject to some human rights obligations even in situations in which it does not exercise full physical control over an individual and the entire corpus of human rights. If it exercises effective control over the ability of the individual to enjoy that right, then the obligation applies extraterritorially*"[44].

Zusammenfassend ist daher festzustellen, dass der internationale Menschenrechtspakt auch auf internetgestützte Überwachungsmaßnahmen anwendbar ist und zwar auch dann, wenn Ausländer auf fremdem Staatsgebiet überwacht werden und die konkreten Überwachungsmaßnahmen außerhalb des eigenen Staatsgebiets vorgenommen werden.

III. Vereinbarkeit von Überwachungsmaßnahmen mit dem Recht auf Schutz der Privatsphäre

Es bleibt nunmehr zu analysieren, inwieweit die von NSA und GCHQ durchgeführten Überwachungsmaßnahmen mit dem IPbpR vereinbar sind. Die Überwachung von Kommunikation stellt einen Eingriff in Art. 17 Abs. 1 IPbpR dar, wonach niemand Eingriffen in die Privatsphäre und den Schriftverkehr ausgesetzt werden darf. Internetkommunikation, Aktivitäten in sozialen Netzwerken und die damit einhergehenden Metadaten und Kommunikationsinhalte fallen unproblematisch in den Schutzbereich des Art 17[45]. Auch stellen Überwachung und Kontrolle von Internetkommunikation einen Eingriff in den Schutzbereich dar. Fraglich ist demnach, ob bzw. wann ein solcher Eingriff willkürlich oder rechtswidrig ist und somit gegen Art. 17 verstößt. Diese Frage ist von dem UN-Menschenrechtsausschuss oder anderen Gerichten hinsichtlich des internationalen Menschenrechtspakts noch nicht bindend entschieden worden. Allerdings können den Stellungnahmen des Menschenrechtsausschusses, anderer UN-Organe[46],

---

[44] Common response of Austria, Liechtenstein, Slovenia and Switzerland to the OHCHR request regarding „The right to privacy in the digital age", Brief vom 9. April 2014.

[45] Vgl. Resolution der UN-Generalversammlung *Right to Privacy in the Digital Age*, UNGA Res. 68/167.

[46] UNHCR, Bericht vom 30 Juni 2014, *The right to privacy in the digital age*, A/HRC/27/37.

sowie v.a. den Entscheidungen des EGMR[47] Kriterien entnommen werden, die einzelne Überwachungsmaßnahmen und die sie autorisierenden Gesetze erfüllen müssen, um rechtskonform zu sein. Diese Kriterien beziehen sich auf die Qualität der Eingriffsnorm, die Dauer und Intensität der Überwachung, die Verfügbarkeit effektiven Rechtschutzes und die Verhältnismäßigkeit und Notwendigkeit der Maßnahme.

So muss das die Überwachung erlaubende und somit Art. 17 IPbpR beschränkende Gesetz zugänglich und transparent (*accessible and transparent*)[48] sein; der Bürger muss zudem dem Gesetz entnehmen können, unter welchen Umständen der Staat die Kommunikation der Bürger überwachen kann[49]. Die Überwachung darf nicht anhaltslos sein, vielmehr muss das Gesetz die genauen Umstände benennen und die Überwachung auf den Verdacht bestimmter und konkret bestimmbarer Straftaten beschränken, sodass die Öffentlichkeit die Natur der Handlungen, die zu einer Überwachung führen, verstehen kann[50]. Wird die Überwachung anhand von Selektoren bzw. anderen Auswahlkriterien geführt, müssen diese in einer Form benannt werden, die der Öffentlichkeit Zugang und Kontrolle (*open to public scrutiny and knowledge*) ermöglicht[51]. Die Überwachungsmaßnahmen müssen zudem zeitlich beschränkt sein. Das Gesetz muss den Zeitpunkt festlegen, nach dem die Erlaubnis zur Überwachung ausläuft, sowie die Voraussetzungen für ihre Verlängerung und Umstände benennen, die ihre sofortige Beendigung erfordern[52]. Zudem muss das Gesetz die Speicherung der gesammelten Daten auf einen vernünftigen Zeitraum, der den Umständen angemessen ist, begrenzen[53]. Offensichtlich irrelevante Daten müssen sofort gelöscht werden[54]. Den überwachten Personen muss ein effektiver Rechtschutz gewährleistet werden, der u.U. auch bedeutet, dass eine überwachte Person nach Beendigung der Überwachung darüber informiert werden muss[55]. Schließlich muss die Überwachung auch verhältnismäßig sein, d.h. ein

---

47 EGMR, Urteil vom 29. Juni 2006, *Weber und Saravia v. Deutschland*, Az. 54934/00; EGMR, Urteil vom 6. September 1978, Az. 5029/71, *Klass u.a. v. Deutschland*; EGMR, Urteil vom 1. Juli 2008, Az. 58243/00, Liberty v. UK; EGMR, Urteil vom 4. Dezember 2015, Az. 47143/06, *Zakharov v. Russland*; EGMR, Urteil vom 12. Januar 2016, Az. 37138/14, *Szabo und Vissy v. Ungarn*.

48 EGMR, *Weber und Saravia*, Rn. 84.

49 EGMR, *Weber und Saravia*, Rn. 93.

50 EGMR, *Weber und Saravia v. Deutschland*, Rn. 95; EGMR, *Zakharov v. Russland*, Rn. 248.

51 EGMR, *Liberty v. UK*, Rn. 67.

52 EGMR, *Zakharov v. Russland*, Rn. 250.

53 EGMR, *Zakharov v. Russland*, Rn. 253–256.

54 EGMR, *Zakharov v. Russland*, Rn. 255.

55 EGMR, *Weber und Saravia v. Deutschland*, Rn. 135.

legitimes Ziel verfolgen[56], angemessen[57] und erforderlich sein[58]. Insbesondere muss die Überwachungsmaßnahme gegen eine konkrete, klar identifizierbare Person gerichtet sein[59].

Nach den oben skizzierten Kriterien ist klar, dass die vom NSA und GCHQ geführten Überwachungsprogramme die rechtlichen Anforderungen des Art. 17 IPbpR (und auch des Art. 8 EGMR) nicht erfüllen und die Staaten ihre Fernmeldeaufklärungsprogramme an die benannten Kriterien anpassen müssen.

IV. Schlussfolgerungen

Das digitale Zeitalter und die mit ihm einhergehenden Möglichkeiten und Gefahren machen eine Neuregelung des Verhältnisses zwischen dem Bedürfnis nach Sicherheit und der daraus entspringenden staatlichen Kontrolle einerseits und dem Recht auf Schutz der Privatsphäre im Onlinebereich notwendig. Klar ist, dass die Staaten in ihren Handlungen im Internet nicht mehr zwischen (strikt regulierten) Inlands- und (wenig regulierten) Auslandsaktivitäten unterscheiden dürfen, sondern aufgrund ihrer internationalen Verpflichtungen dieselben Rechte In- und Ausländern zukommen lassen müssen. Klar ist aber auch, dass die Gefahren, die aus der Nutzung moderner Kommunikationstechnologien durch Terroristen entspringen, einen absoluten Rückzug des Staates aus dem Onlinebereich nicht erlauben. Den ständigen Konflikt zwischen Sicherheit und Freiheit im Onlinebereich so zu lösen, dass effektive Sicherheit bei maximaler Grundrechtsachtung gewährleistet werden kann, wird eine der großen Herausforderungen für Gesetzgeber, Gerichte und das Völkerrecht im 21. Jahrhundert sein.

---

[56] EGMR, *Weber und Saravia v. Deutschland*, Rn. 107; M. Milanovic, *Human Rights*, S. 136; UNHCHR Bericht Rn. 23.

[57] EGMR, *Weber und Saravia v. Deutschland*, Rn. 107; UNHCHR Bericht, Rn. 25.

[58] EGMR, *Weber und Saravia v. Deutschland*, Rn. 105; UNHCHR Bericht, Rn. 22.

[59] EGMR, *Zakharov v. Russland*, Rn. 264.