Z Außen Sicherheitspolit (2015) 8:447–459
DOI 10.1007/s12399-015-0529-x

ANALYSE

Globale Überwachung und digitale Souveränität

Peter Schaar

Online publiziert: 16. September 2015

Zusammenfassung Die Überwachungstätigkeiten der NSA und ihres Partners GCHQ sind global ausgelegt und daher nur schwer rechtlich zu begrenzen. Dadurch gerät der Grundrechtsschutz in Gefahr. Es muss daher diskutiert werden, inwieweit die globalen Überwachungsaktivitäten die nationale Souveränität der betroffenen Staaten berühren. Dieser Beitrag wendet die Souveränität als völkerrechtliche Kategorie auf den Digitalraum an und kommt zu dem Schluss, dass das Territorialprinzip, der Datenschutz und die Freiheit im Internetzeitalter neuen Herausforderungen ausgesetzt sind.

Schlüsselwörter Strategische Kommunikationsaufklärung · Internetkommunikation · Souveränität · Datenschutz · Grundrechtsschutz

Global Surveillance and Digital Sovereignty

Abstract The surveillance operations of the NSA and its partner GCHQ are pursued on a global scale and target transnational internet communications. This makes it difficult to constrain surveillance activities through national legislation. Therefore there is an ongoing discussion about the role of sovereignty in the digital realm. This contribution discusses the applicability of this principle to the cyber domain and concludes that the categories of territory, data-protection and freedom are at stake.

P. Schaar (✉)
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit a. D.,
Europäische Akademie für Informationsfreiheit und Datenschutz (EAID),
Bismarckallee 46/48,
14193 Berlin, Deutschland
E-Mail: schaar@eaid-berlin.de

Keywords Signals intelligence · Internet communication · Sovereignty · Data-protection · Rights protection

1 Digitalisierung und nationales Recht

Die durch Edward Snowden bekannt gemachten internen Unterlagen des US-Nachrichtendienstes National Security Agency (NSA), daran anknüpfende Recherchen investigativer JournalistInnen und die Arbeit parlamentarischer Untersuchungsausschüsse vermitteln das Bild von Geheimdiensten, die insbesondere bei der sogenannten Auslandsaufklärung keinen rechtlichen und kaum faktischen Schranken begegnen. Die Überwachungsaktivitäten sind global und an ihnen wirken nicht nur die NSA und ihr britischer Konterpart Government Communications Headquarters (GCHQ) mit. Auch die Geheimdienste vieler anderer Staaten, offenbar auch der deutsche Bundesnachrichtendienst (BND), sammeln in ungeheurem Umfang digitale Daten und überwachen Kommunikationsvorgänge. Technische Mittel, Rohdaten und bei der Überwachung gewonnene Erkenntnisse werden recht freizügig mit den jeweils *befreundeten* Diensten geteilt, in der Hoffnung darauf, im Gegenzug an den Früchten der internationalen Überwachung durch andere Dienste zu partizipieren.

Immer deutlicher wird dabei, dass Rechtsvorschriften, die in den westlichen Demokratien die Aufgaben und Befugnisse der Nachrichtendienste festlegen, gegenüber der globalen, kooperativ durchgeführten Auslandsüberwachung kaum Wirkung entfalten. Zum einen beschränken sich die Regelungen des nationalen Rechts zum Grundrechtsschutz im Wesentlichen auf die Begrenzung der Inlandsüberwachung und der Ausforschung jeweils eigener StaatsbürgerInnen im Ausland. Hinsichtlich der Ausforschung ausländischer Rechtssubjekte – Firmen und Personen – orientieren sich die Dienste am jeweiligen, naturgemäß weit gefassten *nationalen Interesse*. So sieht sich etwa der Bundesnachrichtendienst bei seiner Auslandsüberwachung nicht an die im Grundgesetz (GG) festgeschriebenen Grundrechte gebunden, etwa an das Fernmeldegeheimnis (Art. 10 GG). Offenbar gilt dies auch für die Vorgabe, es gehöre zur „verfassungsrechtlichen Identität der Bundesrepublik Deutschland […], dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf“ (Bundesverfassungsgericht 2010), jedenfalls soweit es sich um die Erfassung und Registrierung der Auslandskommunikation handelt, selbst wenn die entsprechenden Überwachungsaktivitäten innerhalb Deutschlands stattfinden.

Digitalisierung und globale Informationsnetze, datengetriebene Geschäftsmodelle und elektronische Dienstleistungen führen zu immer umfangreicheren grenzüberschreitenden Datenströmen. Dabei werden Daten häufig auch bei solchen Kommunikationsvorgängen über ausländische Server und Netzknoten geleitet, an denen ausschließlich inländische Kommunikationspartner teilnehmen. Eine trennscharfe Unterscheidung von Inlands- und Auslandskommunikation ist häufig kaum möglich. Zudem sehen sich ausländische Nachrichtendienste, die auf ihrem Territorium auf ausländische (Transit-)Daten zugreifen, regelmäßig nicht an die rechtlichen Restriktionen gebunden, die sie bei der Inlandsüberwachung zu beachten haben.

Weiterhin beschränken inländische Rechtsvorschriften – etwa das Fernmeldegeheimnis nach Art. 10 GG – die Überwachungsaktivitäten ausländischer Nach-

richtendienste nicht, soweit sie im Ausland, im Weltraum, bei Funkübertragungen, an Netzknoten oder auf hoher See durch Anzapfen von Überseekabeln stattfinden. Deutsches Recht hindert etwa die amerikanischen Geheimdienste nicht daran, die gewonnenen Daten und Erkenntnisse mit anderen ausländischen Diensten zu teilen, soweit sie der Auffassung sind, dass dies im nationalen Interesse der USA liegt. Den Empfängern – auch den deutschen Nachrichtendiensten – fließen so Informationen mit Inlandsbezug zu, die sie selbst nicht hätten erheben dürfen.

Durch die nachrichtendienstliche Auslandsüberwachung und den gegenseitigen Informationsaustausch werden im Ergebnis die durch nationales Recht verbürgten Grundrechte unterminiert oder umgangen. In diesem Kontext sind die Vorwürfe gegen den BND zu verstehen, von US-Diensten gelieferte Selektoren bei der Überwachung der Satellitenkommunikation und der leitungsgebundenen Transitkommunikation zu verwenden, die europäische Unternehmen, EU-Institutionen und PolitikerInnen anderer Mitgliedsstaaten betreffen. Dabei handelt es sich um Suchbegriffe, die als Kriterien für die gezielte Erfassung der Kommunikationsvorgänge herangezogen werden (Biermann und Beuth 2015).

Viele der bei der Auslandsüberwachung gewonnenen Daten hatte der BND offenbar an die US-Dienste weitergegeben, wie die Bundesregierung bereits im August 2013 bestätigte:

> Die Kooperation mit anderen Nachrichtendiensten findet auf gesetzlicher Grundlage statt. Metadaten aus Auslandsverkehren werden auf der Grundlage des Gesetzes über den Bundesnachrichtendienst (BND-Gesetz) an ausländische Stellen weitergeleitet. Vor der Weiterleitung werden diese Daten in einem gestuften Verfahren um eventuell darin enthaltene personenbezogene Daten deutscher Staatsbürger bereinigt. (Deutscher Bundestag 2013, S. 8)

Bemerkenswert war an diesem Eingeständnis nicht nur, dass der BND millionenfach vertrauliche Daten sammelt. Noch bedenklicher ist es, dass der deutsche Auslandsnachrichtendienst diese Daten in großem Umfang an die NSA weiterleitete. Angesichts der riesigen Datenmengen, die übermittelt werden, ist nicht vorstellbar, dass der BND im Einzelfall prüfte, ob die Voraussetzungen für eine Datenübermittlung vorlagen. Auch der Hinweis der Bundesregierung, dass vor der Übermittlung diejenigen Daten, die deutsche Kommunikationsteilnehmende betreffen, vor der Übermittlung herausgefiltert würden, beruhigte nicht wirklich. Denn weder Telefonnummern noch die E-Mail-Kennungen ermöglichen eine sichere Unterscheidung nach Staatsangehörigkeit und Land. Wie soll es dem BND etwa möglich sein, die Daten eines deutschen Nutzers herauszufiltern, der in seinem Mobiltelefon eine ausländische Simkarte benutzt oder Kunde bei einem internationalen E-Mail-Anbieter ist, dessen Domainname auf *.com* und nicht auf *.de* endet? Zudem werden die Daten von BürgerInnen anderer EU-Staaten offenbar nicht aus dem Bestand ausgefiltert – jedenfalls ist davon in der Antwort der Bundesregierung nicht die Rede.

Auch wenn es sich bei der globalen Überwachung um ein Geschäft auf Gegenseitigkeit handelt, ist wiederholt die Frage aufgetaucht, inwieweit die globalen Überwachungsaktivitäten die nationale Souveränität der betroffenen Staaten berühren. In vielen Staaten – auch in Deutschland – werden die Rufe nach der Gewährleistung

einer *digitalen Souveränität* lauter. Inländische Personen, Firmen oder Institutionen sollen vor ausländischen Überwachungsaktivitäten wirksam geschützt werden. Gemeint werden damit unterschiedliche Aspekte:

1. Die eigenen Nachrichtendienste erhalten zusätzliche Überwachungsbefugnisse und sie werden personell und technisch verstärkt, um sie auf *Augenhöhe* mit den als weltweit führend angesehenen Diensten der USA und Großbritanniens (und vielleicht Chinas) zu bringen. Die für die geheimdienstliche Aufrüstung vorgebrachte Warnung vor *Cybergefahren* bezieht sich in Wirklichkeit nicht nur und vermutlich nicht einmal vorrangig auf Kriminelle oder terroristische Gruppen, sondern auf fremde Nachrichtendienste.
2. Angesichts der vermuteten und teils nachgewiesenen Hintertüren in Hard- und Software wird gefordert, die Abhängigkeit von wenigen, ganz überwiegend in den USA und China ansässigen Herstellern zu überwinden. Gezielte Förderprogramme eigener Unternehmen und entsprechende Anforderungen bei der Beschaffung von IT-Komponenten sollen zumindest in Kernbereichen die technologische Souveränität ermöglichen (Eckert 2013).
3. Des Weiteren wird gefordert, die Unabhängigkeit der eigenen Telekommunikationsnetze einschließlich des Internets von ausländischen (namentlich amerikanischen) Anbietern herzustellen. Die Netz- und Serverstrukturen sollen so gestaltet werden, dass die im Inland generierten Daten die entsprechenden Territorien nicht verlassen. In verschiedenen Staaten gibt es Bestrebungen, Firmen, öffentliche Stellen und sogar PrivatnutzerInnen zu verpflichten, ihre Datenhaltung ausschließlich im Inland bzw. der entsprechenden Region vorzunehmen.

2 Die digitale Dimension der Souveränität

Souveränität als völkerrechtliche Kategorie bezeichnet die auf faktischer Herrschaft beruhende staatliche Unabhängigkeit. Souveräne Staaten bestimmen ihre rechtliche, wirtschaftliche und politische Ordnung selbst. Vor dem Völkerrecht sind alle Staaten gleich – unabhängig von tatsächlichen Machtunterschieden. Eingriffe anderer Staaten in die nationale Souveränität sind völkerrechtlich unzulässig, soweit nicht das Völkerrecht selbst solche Eingriffe rechtfertigt. Souveränität ist traditionell territorial definiert, im Hinblick auf die tatsächliche Ausübung von Herrschaft. Dabei wurden nicht nur die jeweiligen Landmassen, sondern auch die umschlossenen Gewässer und die angrenzenden Seegebiete (maximal 12 Seemeilen vom Ufer – *Küstenmeer*) als nationales Territorium angesehen.

In Bezug auf die digitale Souveränität drängt sich eine Analogie zum Luftrecht auf, denn auch hier ging es um eine neue Dimension, die bei den territorial orientierten Souveränitätskonzepten zunächst nicht im Blick war. Mit dem Aufkommen der Luftfahrt Ende des 19. Jahrhunderts und der Weltraumfahrt in der zweiten Hälfte des 20. Jahrhunderts stellte sich die Frage, wie weit die Souveränität vertikal reicht und wie sich die Souveränitätssphären der Staaten gegeneinander abgrenzen lassen. Diese Aufgabe ließ sich prinzipiell leicht lösen, indem man den Luftraum über dem Hoheitsgebiet grundsätzlich dem jeweiligen Staatsgebiet zuordnete. Unumstritten ist

inzwischen, dass der Raum oberhalb von 120 km, also der untersten möglichen Satellitenlaufbahn, dem Weltraum zuzurechnen ist (Epping 2014, S. 52). Der Weltraum ist exterritorial; seine Nutzung steht jedem Staat frei, wird allerdings durch völkerrechtliche Regelungen normiert, insbesondere dem UN-Weltraumvertrag von 1966. Dieser stellt allerdings klar, dass die Nutzung in Übereinstimmung mit dem Völkerrecht zu erfolgen hat (Vereinte Nationen 1966, Art. I). Souveränitätsansprüche bestehen im Hinblick auf die von den Staaten betriebenen eigenen Satelliten, unabhängig von deren Umlaufhöhe und der Umlaufbahn.

Die Frage, wie weit die aus dem Weltraum erhobenen Daten verwendet werden dürfen, ist Gegenstand der von der UN-Generalversammlung im Konsens angenommenen Fernerkundungsresolution 41/65 vom 03.12.1986. Danach haben alle Staaten ein Recht auf Fernerkundung, ohne die ausgekundschafteten Staaten um Erlaubnis bitten zu müssen (Heintze 2014, S. 977).

Zudem betrachten es Geheimdienste in aller Welt offenbar als Gewohnheitsrecht, per Funk (terrestrisch oder per Satellit) übertragene Daten mitzulesen und auszuwerten. Insbesondere während des Kalten Kriegs in den 1950er und 1960er Jahren wurden die im *Ätherraum* übertragenen Signale systematisch abgehört und aufgezeichnet. Die Verbreitung von Funksignalen lässt sich nicht auf bestimmte Territorien eingrenzen und sie lassen sich mit entsprechender Technik auch fernab der eigentlichen Zielgebiete abfangen und auswerten. Dies gilt für sämtliche Arten der Funkkommunikation: für militärische und zivile Funkgeräte genauso wie für moderne Mobilfunksysteme und für die Satellitenkommunikation. Das geteilte Deutschland war während des Kalten Kriegs in den 1950er bis 1970er Jahren ein zentrales Feld zur Beschaffung von Signals Intelligence (SIGINT). Dabei ging es zunächst in erster Linie nicht um das Ausspionieren einzelner Personen. Im Mittelpunkt dieser strategischen Überwachung standen Erkenntnisse militärischer Aktivitäten der Gegenseite, deren Planungen und das jeweilige Umfeld. Ökonomische Daten waren ebenso von Interesse wie politische Stimmungen und Einschätzungen.

Erst in den 1990er Jahren, also erst nach Beendigung der Blockkonfrontation, ist bekannt geworden, dass westliche Geheimdienste systematisch die mittels Fernmeldesatelliten übertragene Kommunikation überwachten. Das wichtigste Instrument war dabei das von der NSA zusammen mit befreundeten Nachrichtendiensten unter dem Decknamen ECHELON betriebene Projekt, ein weltumspannendes Netz von Stationen zur Überwachung der Satellitenkommunikation. 1998 bestätigte eine im Auftrag des Europäischen Parlaments erstellte Studie den Verdacht, dass sich die Überwachung nicht auf die Satelliten beschränkte, sondern auch andere Übertragungswege umfasste, insbesondere die mittels Kabel betriebenen Telekommunikationsnetze. Sämtliche Kommunikation via E-Mail, Telefon und Fax werde von der NSA routinemäßig überwacht – auch innerhalb Europas (EP 2002).

Seither hat sich die Welt der Telekommunikation drastisch verändert. Die Bedeutung der Satellitentechnik im Fernmeldeverkehr hat stark abgenommen. Der bei weitem bedeutendste Teil der globalen Kommunikation wird heute über Glasfaserkabel abgewickelt. Praktisch die gesamte elektronische Kommunikation – auch der Telefonverkehr – läuft heute über die durch das Internet bereitgestellte Infrastruktur. Wegen dieser technischen Änderungen konzentrieren sich die geheimdienstlichen Überwachungsaktivitäten heute auf das Internet. Glasfaserkabel, Verstärkereinrich-

tungen, Netzknoten, Server und Endgeräte werden überwacht. Die Überwachungsaktivitäten lassen sich deshalb – anders als bei der Überwachung des *Ätherraums* – überwiegend räumlich zuordnen, je nachdem wo die entsprechenden Ausleitungen stattfinden.

Im Hinblick auf die Souveränitätsrechte stellt das Überwachen von Unterseekabeln einen Sonderfall dar, jedenfalls soweit der Zugriff außerhalb nationaler Hoheitsgebiete stattfindet. Hier stellt sich die Frage, inwieweit die Überwachung gegen die Prinzipien der Nutzung des Meeresbodens verstößt, der ebenso wie der Weltraum als gemeinsames Erbe der Menschheit angesehen wird, auf das kein Staat einen Souveränitätsanspruch erheben darf. Zu den zulässigen Nutzungen des Meeresbodens gehört das Recht eines jeden Staats, Kabel oder Rohrleitungen zu verlegen. Zugleich ist es ihnen verboten, fremde Kabel zu unterbrechen oder zu beschädigen (Vereinte Nationen 1958, Art. 26, 1), sodass sich die Frage aufdrängt, ob ein heimliches Anzapfen transatlantischer Glasfaserkabel, das regelmäßig mit deren Beschädigung verbunden ist, einen völkerrechtswidrigen Eingriff darstellt.

Insbesondere der britische Geheimdienst hat sich bei der Überwachung der Unterwasserkabel hervorgetan, wie wir inzwischen auf Grund der Snowden-Papiere wissen. Der Computergeheimdienst GCHQ verschaffte sich unter dem Codewort *Tempora* systematisch Zugang zu Glasfaserkabeln (mehr als 200), die Europa mit den Vereinigten Staaten und mit anderen Weltregionen verbinden (The Guardian 2013). Für die Überwachung der Unterseekabel nutzt der GCHQ seine Zugangsmöglichkeiten zu Relaisstationen, in denen die übertragenen Signale verstärkt werden. Die Betreiber der Stationen sind zur Zusammenarbeit mit dem britischen Geheimdienst verpflichtet. Außerdem ist es den Briten offenbar gelungen, auch in Küstennähe verlaufende Verbindungen anzuzapfen. Ob der GCHQ sich dabei – wie öffentlich spekuliert wird (Spiegel Online 2013) – im Wege der Amtshilfe amerikanischer Spezial-U-Boote bedient, die nach Einschätzung von GeheimdienstexpertInnen in der Lage sind, Unterwasserkabel anzuzapfen, ist nicht nachgewiesen.

Seit den Snowden-Veröffentlichungen ist offensichtlich, dass sich die herkömmlichen Vorstellungen von Souveränität nicht ohne weiteres in den Cyberspace übertragen lassen. Von Souveränität kann nur gesprochen werden, wenn die Durchsetzung des Rechts auch tatsächlich erfolgen kann. Dies ist aber bei den derzeitigen Netz- und Informationsstrukturen schwer vorstellbar.

Während bei der Festlegung des Bereichs, der von der Souveränität umfasst wird, im realen Raum nachvollziehbare Kriterien zur Verfügung stehen – auch wenn sie im Einzelfall umstritten sein mögen – fehlen derartige Messgrößen im virtuellen Raum der globalen Informationsverarbeitung. Auch wenn die meisten Datenverarbeitungsvorgänge irgendwelche territorialen Anknüpfungspunkte haben – schließlich müssen die Server, Leitungen, Netzknoten und Endgeräte irgendwo betrieben werden und auch bei Satellitenverbindungen gibt es terrestrische Sende- und Empfangseinrichtungen – entzieht sich die komplexe, vielfach vernetzte Informationsverarbeitung in einem globalen Raum. Daten können per Mausklick in einen anderen Kontinent verschoben oder von dort abgerufen werden. Die De-Lokalisierung der Informationsverarbeitung *(cloud computing)* wird als Lösung vielfältiger Probleme propagiert und erfreut sich zunehmender Beliebtheit. Der Nutzer, aber auch der für die Daten eigentlich Verantwortliche haben kaum noch Einfluss darauf, wo die Daten tatsächlich

verarbeitet werden. Vielfach ist es ihnen zudem völlig unmöglich herauszufinden, auf welchen Servern in welchem Land sich die jeweiligen Informationen physisch befinden.

Gleichwohl knüpfen die rechtlichen Vorgaben zur Regulierung und Überwachung im nationalen Recht zumeist an der Lokalität der zur Informationsverarbeitung betriebenen Technik an. Netzknoten werden mit Überwachungsschnittstellen ausgestattet und die Betreiber zur heimlichen Ausleitung der Daten an Geheimdienste und/oder Strafverfolgungsbehörden verpflichtet. Router und andere IT-Komponenten werden mit Hintertüren ausgestattet, die den staatlichen Bedarfsträgern und ggf. anderen Dritten Zugriff auf die verarbeiteten Daten geben.

Von besonderem Interesse ist schließlich die Forderung nationaler Behörden, von Unternehmen die Herausgabe von Daten auch dann zu verlangen, wenn diese außerhalb des eigenen Hoheitsgebiets gespeichert sind. Im Frühjahr 2014 verurteilte ein New Yorker Bundesrichter die Firma Microsoft, US-Sicherheitsbehörden auch dann Zugang zu E-Mails und anderen elektronisch gespeicherten Informationen geben zu müssen, wenn diese nicht auf Servern in den Vereinigten Staaten, sondern im Ausland gespeichert sind (Reuters 2014). Die KundInnen von US-Unternehmen, die ihre Daten etwa in einer Cloud speichern, müssen danach davon ausgehen, dass ihre Daten dem Zugriff durch US-Behörden nach amerikanischem Recht ausgesetzt sind. Damit gelangen die US-Behörden an im Ausland gespeicherte Daten, für die sie ansonsten den Weg der internationalen Rechtshilfe begehen müssten. Dies widerspricht internationalem Recht. Ein solcher exterritorialer Datenzugriff ist insbesondere deshalb problematisch, weil die Daten von Personen, die sich nicht dauerhaft in den USA aufhalten, nach US-Recht kaum gesetzlich geschützt sind. Betroffene EU-BürgerInnen und andere AusländerInnen haben bislang nicht einmal das Recht, vor US-Gerichten gegen die Praktiken amerikanischer Behörden beim Umgang mit ihren Daten zu klagen. Mit seiner Entscheidung durchkreuzte das Gericht die von einigen US-Unternehmen unternommenen Anstrengungen, ausländischen KundInnen sichere und vertrauenswürdige Internet-Dienste anzubieten, die durch das jeweilige nationale bzw. europäische Recht geschützt sind. So hatte die Firma IBM vor kurzem angekündigt, in Deutschland ein neues Rechenzentrum zu errichten, in dem die Daten „unter Einhaltung sämtlicher Datenschutzvorgaben aus Deutschland und der EU ins Netzwerk aufgenommen werden“ (Werlin 2014).

3 Grundrechtsbindung bei der nachrichtendienstlichen Auslandsaufklärung

Die nationale Souveränität hat zwei Seiten. Sie wirkt einerseits extern gegenüber anderen Staaten und ist Gegenstand des Völkerrechts. Vergessen werden darf aber andererseits nicht, dass sie auch eine interne Wirkung bezüglich derjenigen Rechtssubjekte entfaltet, die im eigenen Hoheitsgebiet agieren oder in staatlichem Auftrag – auch im Ausland – tätig sind.

Dass dies nicht unstrittig ist, zeigen die Verhandlungen des parlamentarischen Untersuchungsausschusses des Deutschen Bundestags zur NSA-Affäre. Die BND-Führung war offenbar der Auffassung, dass der durch Art. 10 GG gewährleistete Schutz des Fernmeldegeheimnisses nicht für die Überwachung der Auslandskom-

munikation gelte, selbst wenn die Überwachung von deutschem Boden aus erfolgt und/oder die erlangten Daten in Deutschland verarbeitet werden (Krempl 2014). Nach der BND-Rechtsauffassung ermächtige die allgemeine Aufgabenzuweisung zur Auslandsaufklärung im BND-Gesetz den Dienst zur Auslandsüberwachung von Telefonaten und Internetverkehren, auch wenn eine explizite Einschränkung von Art. 10 GG durch das Gesetz nicht erfolge. Demgegenüber haben die vom NSA-Untersuchungsausschuss des Deutschen Bundestags geladenen Sachverständigen einhellig die Auffassung vertreten, dass der Schutzbereich von Art. 10 GG auch die Auslandskommunikation umfasse.

So stellte etwa der ehemalige Präsident des Bundesverfassungsgerichts Prof. Hans-Jürgen Papier in seinem Gutachten für den Untersuchungsausschuss fest:

> Deutsche Behörden, einschließlich der Nachrichtendienste, sind an Art. 10 GG auch dann gebunden, wenn und soweit sie die grenzüberschreitende Telekommunikation überwachen. Art. 10 GG schützt als Menschenrecht und damit gemäß seinem weiten personellen Schutzbereich nicht nur Deutsche sondern auch Ausländer. Das gilt uneingeschränkt für die Telekommunikationsverkehre von Deutschen und Ausländern im deutschen Staatsgebiet, aber auch für solche, bei denen ein Endpunkt im Ausland, der andere im Inland liegt. Sofern beide Endpunkte des Telekommunikationsverkehrs im Ausland liegen, sind die den Eingriff in das Telekommunikationsgeheimnis vornehmenden deutschen Behörden grundsätzlich ebenfalls an Art. 10 GG gebunden; der räumliche Schutzumfang des Fernmeldegeheimnisses ist also nicht auf das Inland begrenzt (BVerfGE 100, 313). Das gilt nach der Rechtsprechung des Bundesverfassungsgerichts jedenfalls dann, wenn eine im Ausland stattfindende Telekommunikation durch Erfassung und Auswertung im Inland hinreichend mit inländischem staatlichen Handeln verknüpft ist. (Papier 2014, S. 7)

Die beiden anderen Sachverständigen, der ehemalige Bundesverfassungsrichter Prof. Hoffmann-Riem und Prof. Matthias Bäcker kamen ebenfalls zu dem Ergebnis, dass Art. 10 GG vom BND auch bei der Überwachung der Telekommunikation im Ausland zu beachten sei und dass der Dienst deshalb eine gesetzliche Ermächtigung für diese Aktivitäten benötige.

Völlig unhaltbar ist jedenfalls die Position, dass Überwachungsaktivitäten von BND-MitarbeiterInnen auf deutschem Boden keinen Eingriff in das Fernmeldegeheimnis darstellen. Dazu gehören auch die Auswertung und weitere Verarbeitung der durch Überwachung gewonnenen Daten einschließlich deren Weitergabe an ausländische Geheimdienste. Insofern kann und sollte der Bundestag den weitgehend ungeregelten Überwachungsaktivitäten des deutschen Auslandsgeheimdienstes durchaus klare Grenzen setzen. In den Regeln müssen – unter Beachtung der Grund- und Menschenrechte – sowohl die sachlichen Voraussetzungen für die Überwachung bestimmt als auch wirksame parlamentarische, datenschutzrechtliche und gerichtliche Kontrollmechanismen festgelegt werden. Der Zustand, dass der BND hier bisher ohne entsprechende Schranken handelt, ist jetzt – nachdem das Ausmaß der Überwachung immer deutlicher geworden ist – auf keinen Fall mehr hinzunehmen.

Doch selbst für den jeweiligen Heimatstaat, der die Befugnisse der Auslandsgeheimdienste zur Telekommunikationsüberwachung und zur Datengewinnung gesetzlich normiert, bedeutet dies keinesfalls, dass damit die Überwachung im Zielland nach dessen Recht rechtmäßig wäre. Dies gilt etwa für die am 2. Juni 2015 vom US-Kongress beschlossene Geheimdienstreform. Der USA Freedom Act erlaubt der NSA und den anderen US-Geheimdiensten zwar weiterhin eine sehr umfassende Auslandsüberwachung, legt ihnen aber gewisse Fesseln an, etwa indem er auch bestimmte nachrichtendienstliche Auslandsaktivitäten und die Verwendung der dabei gewonnenen personenbezogenen Daten grundsätzlich an einen Richtervorbehalt binden.

4 Globale Überwachung und Territorialprinzip

Geheimdienste, die sich bei ihren Aktivitäten im Ausland verdeckter Mittel bedienen, geraten regelmäßig in Konflikt mit den dortigen Rechtsordnungen. Spionage ist zwar völkerrechtlich nicht verboten. Trotzdem gelten für Nachrichtendienste die rechtlichen Vorgaben im jeweiligen Operationsgebiet. Kein souveräner Staat erlaubt ausländischen Diensten die gegen die eigenen Interessen gerichtete Spionage.

Einen Sonderfall stellen solche Staaten dar, deren Souveränität eingeschränkt ist, etwa weil sie nach einer militärischen Niederlage unter Besatzungsrecht stehen. Dies galt auch für Deutschland nach dem Zweiten Weltkrieg. Die westlichen Alliierten der damaligen Kriegskoalition (USA, Großbritannien und Frankreich) hatten sich durch verschiedene, überwiegend geheime Abmachungen umfangreiche Vorbehaltsrechte ausbedungen, die ganz überwiegend erst mit der deutschen Wiedervereinigung erloschen. Der Historiker Joseph Foschepoth (2012) hat in seinem Werk über die Überwachung in Westdeutschland anhand inzwischen zugänglicher ehemals geheimer Unterlagen nachgewiesen, wie weit diese Überwachungsvorbehalte gingen und dass sie jedenfalls bis 1990 aufrechterhalten wurden, obwohl mehrere deutsche Kanzler – von Konrad Adenauer bis Willy Brandt – der Öffentlichkeit recht erfolgreich weismachen konnten, dass (West-)Deutschland ein souveräner Staat mit allen Rechten und Pflichten sei. Erst mit der Herstellung der deutschen Einheit 1990 traten die meisten der entsprechenden Befugnisse der Westalliierten zur Überwachung in Deutschland außer Kraft.

Unabhängig davon sind immer noch geheime Abmachungen zur geheimdienstlichen Kooperation zu sehen, die nach 1990 und insbesondere nach 2001 abgeschlossen wurden, mit denen sich etwa der NSA-Untersuchungsausschuss befasst. Gleichwohl müssen sich auch danach *befreundete* Nachrichtendienste in Deutschland an deutsches Recht halten. Allerdings sind die Möglichkeiten deutscher Stellen sehr begrenzt, mögliche Rechtsbrüche aufzuklären und die Verantwortlichen zur Rechenschaft zu ziehen. So verletzen die aus Botschaftsgebäuden unternommenen Maßnahmen zur Überwachung des Mobilfunks deutsches Recht. Mangels Zutrittsbefugnis deutscher Datenschutz- und Strafverfolgungsbehörden zu den entsprechenden Liegenschaften ist es aber praktisch nicht möglich, entsprechenden Vorwürfe zu begegnen und die Verantwortlichen strafrechtlich zur Rechenschaft zu ziehen. Dies gilt auch für Überwachungsmaßnahmen, die aus Liegenschaften erfolgen, die den ehemaligen Westalliierten für militärische Zwecke überlassen wurden.

5 Europäische digitale Souveränität?

Als Reaktion auf die Berichte über die insbesondere durch amerikanische Geheimdienste betriebenen globalen Überwachungsmaßnahmen wurde vorgeschlagen, europäische Datenpakete nicht mehr über Netzknoten in Übersee zu senden. So forderten die Datenschutzbeauftragten des Bundes und der Länder, „zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann“ (DSK 2013). Das Internet-Routing sollte so konfiguriert werden, dass die innerhalb eines Gebiets versendeten Nachrichten dieses nicht mehr wie bisher verlassen.

Vor diesem Hintergrund soll der Frage nachgegangen werden, inwieweit man den – auf der Ebene der Nationalstaaten schwer zu realisierenden – Gedanken der digitalen Souveränität auf Europa übertragen kann. Prinzipiell lässt sich die Speicherung und Verarbeitung von Daten in der digitalen Welt eher auf solche geographische Gebiete eingrenzen, die eine entsprechende Größe aufweisen. Niemand würde etwa bezogen auf ein winziges Land wie Luxemburg auf die Idee einer Datenlokalisierung verfallen. Dagegen bestehen in den USA mit ihrer riesigen geographischen Ausdehnung, einem großen Markt und einer weit entwickelten Netzinfrastruktur entsprechende Vorgaben schon seit vielen Jahren. Daten öffentlicher Institutionen müssen in den Vereinigten Staaten gespeichert, verarbeitet und übertragen werden. Auch China bemüht sich mit einigem Erfolg um die elektronische Abwehr und Zensur nicht erwünschter Nachrichten und Dienste (Lee 2015). Insofern sind Bemühungen um europäische Infrastrukturen und entsprechende Vorgaben zur Datenhaltung *(Eurocloud)* nicht von vornherein abwegig. Zudem wäre es bei Gelingen dieses Vorhabens einfacher, die Einhaltung des EU-Datenschutzrechts sicherzustellen.

Technisch ist es heute ohne weiteres möglich, Datenverbindungen, bei denen beide Kommunikationspartner sich in Europa befinden, nur über europäische Netzknoten zu leiten. In den letzten Jahren wurden die europäischen Netzinfrastrukturen massiv ausgebaut, sodass jedes Datenpaket heute auf vielen Wegen innerhalb des Schengen-Raums geroutet werden könnte. Tatsächlich werden aber immer noch viele Datenströme über die USA geleitet – je nach Zeit und Art der Daten und Netzbetreiber bis zu 50 %. Derzeit erfolgt die Wegewahl im Internet im Wesentlichen nach den Kriterien Preis, Entfernung und Service-Qualität. Auch die Ausfallsicherheit des europäischen Netzes ist durch vielfach redundante Verbindungen heute weitgehend gewährleistet. Die Umleitung europäischer Datenpakete über US-Netzknoten hat weniger technische als finanzielle Gründe, denn die US-Anbieter bieten deutlich günstigere Konditionen als die europäische Konkurrenz. Das Routing ausschließlich über europäische Netzkomponenten würde dementsprechend vermutlich zu erhöhten Kosten führen, jedoch kaum mit Einbußen in der Qualität verbunden sein.

Ein zentrales Problem dieses Ansatzes besteht allerdings darin, dass nicht nur die US-Geheimdienste umfassende Lausch- und Überwachungsaktivitäten entfalten, sondern – durch die Snowden-Papiere dokumentiert – auch der britische GCHQ, der sehr eng mit seinem US-Pendant kooperiert. Der zweifelhaften Datenerfassungspraxis des britischen Geheimdienstes wurde mit der Bezugnahme auf den Schengen-Raum, dem Großbritannien nicht angehört, mit der kreativen Sprachschöpfung *Schengen-Routing* Rechnung getragen. Allerdings verdecken solche Sprachkonstruk-

tionen nicht, dass Großbritannien – jedenfalls bis auf weiteres – zur Europäischen Union gehört. Eine digitale Souveränität der EU ohne das Vereinigte Königreich ist kaum denkbar. Bei genauerem Hinsehen erweist sich zudem, dass Großbritannien mit seinen Überwachungsaktivitäten, die auch auf die anderen EU-Mitgliedsstaaten zielen, in Europa nicht allein steht. Nicht zuletzt der BND ist hier in die Kritik geraten (s. o.). Auch die Geheimdienste anderer europäischer Staaten sind bei der Auslandsüberwachung nicht untätig, selbst wenn diese Aktivitäten nicht mit der gleichen Intensität öffentlich debattiert werden. Wer von digitaler Souveränität Europas spricht, darf dies nicht ausblenden.

Selbst wenn es europaweite Vorgaben zum Routing geben würde, würden die Datenströme über den Atlantik nicht automatisch versiegen. Zum einen würden Daten auch weiterhin stets dann in die USA übertragen, wenn die elektronischen Dienstleistungen von dort aus erbracht werden. Dazu kommt, dass amerikanische Anbieter die Daten ihrer NutzerInnen über ihre in den USA gelegenen Infrastrukturen leiten und überwiegend dort auf Servern ablegen. Wer einen amerikanischen E-Mail-Dienst nutzt oder Google als Suchmaschine verwendet, muss also – auch wenn das Schengen-Routing kommen sollte – weiterhin damit rechnen, dass seine Daten in den USA landen, auf dem Weg über Netzknoten und Überseekabel durch den GCHQ und die NSA abgehört und auf Anfrage an US-Sicherheitsbehörden herausgegeben werden. Dies gilt auch für Facebook, das seine Dienste mittlerweile europäischen NutzerInnen offiziell unter der Firma Facebook Ltd. aus Dublin anbietet, denn technisch wird der Dienst weiterhin überwiegend in den USA betrieben.

Schließlich stellt sich die Frage, ob und wie die Praxis der Nachrichtendienste in Europa nach den Maximen der Grund- und Menschenrechte neu geregelt werden könnte. In Verkennung der Rechtslage wird bisweilen von den EU-Gremien verlangt, hier für einen Neuanfang zu sorgen. Politisch wird zwar auch im Europäischen Parlament über die Aktivitäten der Nachrichtendienste der Mitgliedsstaaten diskutiert. Auch die Europäische Agentur für Menschenrechte versucht, sich hier einen Überblick zu verschaffen. Rechtlich sind die Möglichkeiten der EU allerdings beschränkt, denn das europäische Primärrecht konstituiert keinerlei Zuständigkeiten auf dem Gebiet der nationalen Sicherheit. Entsprechende Regelungen sind danach allein Sache der Mitgliedsstaaten. Auf einem Umweg könnte die Europäische Union gleichwohl an der Schnittstelle tätig werden, an der sich staatliche Stellen Zugang zu Informationen verschaffen, die von Unternehmen verarbeitet werden, die am EU-Binnenmarkt teilnehmen. Dies hatte sie bereits bei der 2006 in Kraft getretenen Richtlinie 2006/24/EG zur Vorratsdatenspeicherung praktiziert. Der Europäische Gerichtshof hat in seiner Entscheidung vom 10. Februar 2009 bestätigt, dass die Vorratsdatenspeicherung erheblichen Einfluss auf die im EU-Binnenmarkt tätigen TK-Unternehmen habe und deshalb unter die Binnenmarktkompetenz der EU falle (EuGH 2009). Insofern wäre es – unbeschadet der exklusiven Zuständigkeit der Mitgliedsstaaten für die nationale Sicherheit der EU prinzipiell möglich, den Datenzugriff und die Herausgabeverpflichtung von Unternehmen an Nachrichtendienste europarechtlich zu regeln. Allerdings würde sich die EU auf sehr dünnem Eis bewegen, wenn sie auf diese Weise abseits ausdrücklicher primärrechtlicher Kompetenzen auf die Tätigkeit der Nachrichtendienste Einfluss zu nehmen versuchte.

Deshalb bliebe für eine rechtsstaatliche europaweite Harmonisierung der Arbeit der Nachrichtendienste nur noch der Weg, abseits der EU zu völkerrechtlichen Abmachungen der europäischen Staaten zu kommen. Die Chancen für ein solches Vorhaben dürften sich allerdings – trotz der nicht abreißenden Berichte über globale Überwachungsaktivitäten – in engen Grenzen halten.

6 Fazit

Die Vorstellung einer *digitalen Souveränität* lässt sich rechtlich kaum fassen und stößt daneben auf erhebliche faktische Probleme. Durch Vorgaben zur Lokalisierung der Informationen könnten zwar die Durchsetzungsmöglichkeiten nationalen Rechts verbessert werden, allerdings auf Kosten wesentlicher Vorteile eines globalen Netzes. Insbesondere in autoritär regierten Staaten ist zudem bereits jetzt zu beobachten, dass unter dem Stichwort einer digitalen Souveränität die Meinungs- und Informationsfreiheit eingeschränkt wird. Statt einer informationstechnischen Abkapselung von Staaten und Regionen das Wort zu reden, sollte auf globaler Ebene an der Etablierung datenschutz- und informationsrechtlicher Mindeststandards gearbeitet werden, die unabhängig von der Nationalität oder dem Aufenthaltsort der Betroffenen und der jeweils verwendeten Informations- und Kommunikationstechniken gelten und auch gegenüber den Nachrichtendiensten durchgesetzt werden.

Literatur

Biermann, K., & Beuth, P. (2015, 24. Apr.). Was sind eigentlich Selektoren?. Zeit Online. http://www.zeit.de/digital/datenschutz/2015-04/bundesnachrichtendienst-bnd-nsa-selektoren-eikonal. Zugegriffen: 20. Mai. 2015.

Bundesverfassungsgericht. (2010, 2. März). Urteil vom 02. März 2010–1 BVR 256/08. http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html. Zugegriffen: 7. Aug. 2015.

Deutscher Bundestag. (2013, 14. Aug.). Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD. Abhörprogramme der USA und Umfang der Kooperation der deutschen Nachrichtendienste mit den US-Nachrichtendiensten. Bundestags-Drucksache 17/14560. http://dipbt.bundestag.de/doc/btd/17/145/1714560.pdf. Zugegriffen: 7. Aug. 2015.

DSK – Konferenz der Datenschutzbeauftragten des Bundes und der Länder. (2013, 5. Sep.). Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen. http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/05092013_EntschliessungUeberwachungDurchNachrichtendienste.pdf;jsessionid=C58BD9B9D07CF17B59F7C1A438D8CB8C.1_cid329?__blob=publicationFile&v=1. Zugegriffen: 7. Aug. 2015.

Eckert, C. (2013, 21. Nov.). Digitale Vision für Europa. FAZ.NET. http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/europas-it-projekt/claudia-eckert-fraunhofer-aisec-digitale-vision-fuer-europa-12675295.html. Zugegriffen: 1. Juli. 2015.

EP – Europäisches Parlament. (2002, 21. März). 21. Echelon. A5-0264/2001. Entschließung des Europäischen Parlaments zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) (2001/2098(INI)). Amtsblatt der EU C 72 E/221. http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52001IP0264%2801%29&from=DE. Zugegriffen: 7. Aug. 2015.

Epping, V. (2014). § 5. Der Staat als die „Normalperson“ des Völkerrechts. II. Das Staatsgebiet. In K. Ipsen (Hrsg.), *Völkerrecht, 6., völlig neu bearbeitete Auflage* (S. 50–91). München: C.H. Beck.

EuGH – Gerichtshof der Europäischen Union. (2009, 10. Feb.). Urteil vom 10.02.2009, Irland gegen Europäisches Parlament und Rat der Europäischen Union. Nichtigkeitsklage – Richtlinie 2006/24/EG – Vorratsspeicherung von Daten, die bei der Bereitstellung elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden – Wahl der Rechtsgrundlage. Rechtssache C-301/06. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d511bb25ebd2c74e188cecc94e27553b07.e34KaxiLc3eQc40LaxqMbN4ObN8Ne0?text=&docid=72843&pageIndex=0&doclang=EN-US&mode=lst&dir=&occ=first&part=1&cid=1511375. Zugegriffen: 7. Aug. 2015.

Foschepoth, J. (2012). *ÜberwachtesDeutschland: Post- und Telefonüberwachung in der alten Bundesrepublik*. Göttingen: Vandenhoeck und Ruprecht Verlag.

Heintze, H. (2014). § 48. Weltraumrecht. IV. Einzelfragen der Weltraumnutzung. In K. Ipsen (Hrsg.), *Völkerrecht, 6., völlig neu bearbeitete Auflage* (S. 971–986). München: C.H. Beck.

Krempl, S. (2014, 10. Okt.). NSA-Ausschuss: Streit im BND über massenhafte Datenerfassung. heise online. http://www.heise.de/newsticker/meldung/NSA-Ausschuss-Streit-im-BND-ueber-massenhafte-Datenerfassung-2414969.html. Zugegriffen: 8. Juni 2015.

Lee, F. (2015, 2. Feb.). China schottet sein Internet noch mehr ab. Zeit Online. http://blog.zeit.de/china/2015/02/02/china-schottet-sein-internet-noch-mehr-ab/. Zugegriffen: 4. Feb. 2015.

Papier, H.-J. (2014, 16. Mai). Gutachterliche Stellungnahme Beweisbeschluss des ersten Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode. http://www.bundestag.de/blob/280842/9f755b0c53866c7a95c38428e262ae98/mat_a_sv-2-2-pdf-data.pdf. Zugegriffen: 7. Aug. 2015.

Reuters. (2014, 25. Apr.). U.S. judge rules search warrants extend to overseas email accounts. http://www.reuters.com/article/2014/04/25/us-usa-tech-warrants-idUSBREA3O24P20140425. Zugegriffen: 9. Juni 2015.

Spiegel Online (2013, 1. Juli). Die Datenräuber von der USS ‚Jimmy Carter'. http://www.spiegel.de/forum/politik/nsa-abhoerskandal-die-datenraeuber-von-der-uss-jimmy-carter-thread-94460-1.html. Zugegriffen: 9. Juni 2015.

The Guardian. (2013, 21. Juni). GCHQ taps fibre-optic cables for secret access to world's communications. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. Zugegriffen: 15. Mai 2015.

Vereinte Nationen (1958, 29. Apr.). Convention on the high seas, done at Geneva on 29 April 1958. http://legal.un.org/ilc/texts/instruments/english/conventions/8_1_1958_high_seas.pdf. Zugegriffen: 7. Aug. 2015.

Vereinte Nationen (1966, 19. Dez.). Treaty on principles governing the activities of states in the exploration and use of outer space, including the moon and other celestial bodies. http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html. Zugegriffen: 7. Aug. 2015.

Werlin, B. (2014, 5. Apr.). Neues IBM Smart-Cloud-Rechenzentrum in Ehningen. IT-Zoom. http://www.it-zoom.de/it-director/e/neues-ibm-smart-cloud-rechenzentrum-in-ehningen-5748/. Zugegriffen: 9. Juni 2015.