DIE ÜBERWACHUNG INTERNATIONALER TELEKOMMUNIKATION

HANSJÖRG GEIGER || Der Autor untersucht die verfassungsrechtlichen Probleme, die durch die Aktivitäten von National Security Agency (NSA) und Government Communications Headquarters (GCHQ) und die Zusammenarbeit des Bundesnachrichtendienstes (BND) mit diesen Diensten aufgeworfen wurden. Zentrale Bedeutung hat dabei die Frage, wie weit das Grundrecht des Art. 10 des Grundgesetzes den BND bei der Erfassung und Auswertung von Telekommunikation im Ausland und gegenüber Ausländern bindet und wo gegebenenfalls Bedarf an gesetzlichen Regelungen besteht. Abschließend entwickelt der Autor einige Grundgedanken zum Schutz der Privatsphäre im digitalen Zeitalter.

WAS DÜRFEN DIE DEUTSCHEN NACHRICHTENDIENSTE IN DER TECHNISCHEN AUFKLÄRUNG?

Technische Aufklärung meint Überwachung der Telekommunikation im weitesten Sinne. Die Telekommunikation ist in Deutschland durch Art. 10 GG geschützt. Art. 10 Abs. 1 GG lautet: „Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich."

Das Fernmeldegeheimnis schützt jede Art von Fernmeldeverkehr, also den Fernsprech-, Fernschreib- und auch den Funkverkehr vor Eingriffen. Umfasst sind nicht nur die Inhalte der Kommunikation, sondern auch die Metadaten, also etwa Zeit, Ort, Dauer und die Gesprächspartner.

„Beschränkungen", also Ausnahmen vom Schutz des Fernmeldegeheimnisses, bedürfen eines Gesetzes (Art. 10 Abs. 2 Satz 1 GG), an das angesichts des besonderen Schutzgehalts von Art. 10 GG „in der Regel besonders strenge Anforderungen" zu stellen sind.[1] In diesem Gesetz muss die Einschränkung des Art. 10 GG ausdrücklich genannt sein.

WAS DÜRFEN DIE DEUTSCHEN NACHRICHTENDIENSTE IM RAHMEN DER ÜBERWACHUNG DER TELEKOMMUNIKATION?

In welchem rechtlichen Umfeld haben wir diese Fragestellung zu sehen?

Exkurs: Bundesverfassungsgericht zur Volkszählung und aktuelle Herausforderungen: Wer nicht sicher sein kann, dass seine Aktivitäten staatlich erfasst werden, wird möglicherweise auf die Ausübung seiner demokratischen Rechte verzichten. Aber dies wäre eine Gefahr für die Demokratie.

Damals, also im Jahr 1983, ging es nur um ein paar Daten, heute verbreiten wir ständig, etwa durch die Nutzung der neuen Medien, große Datenmengen über uns. Daraus lassen sich, wie wir alle wissen, detaillierte Persönlichkeitsbilder erstellen. Dies kann etwa bis zur Feststellung der politischen, aber auch der sexuellen Präferenzen der Einzelnen gehen. Das ist der Marktwert, den wir heute großen Internet-Konzernen schenken, wenn wir deren meist unentgeltliche Dienste nutzen.

Diese Entwicklung kann nicht nur zur politischen Enthaltsamkeit führen, daneben sehe ich das fast noch größere Risiko unserer Entmündigung. Facebook und Google bieten personalisierte Antworten auf unsere Fragen. Wir werden in einen Kokon der angeblich von uns erwarteten Antworten gehüllt. Und der angekündigte „persönliche Assistent" wird uns durch das Leben führen, uns die alltäglichen Entscheidungen praktischerweise abnehmen und so unserer Fähigkeit berauben, unser Leben selbstgestaltet zu führen. Nicht zu vergessen, Art. 2 GG garantiert doch ausdrücklich das Recht auf freie Entfaltung der Persönlichkeit. Aber wenn wir aus vermeintlicher Bequemlichkeit darauf verzichten, hilft uns auch das Grundgesetz nicht. Wir verlieren unsere Kreativität, also das, was den Menschen eigentlich ausmacht. Gesichtserkennung und die Datenbrille Google-Glass drohen uns den Rest von Privatheit und Anonymität zu rauben. Ohne die Möglichkeit, sich zurückziehen zu können, allein zu sein, drohen uns seelische Gefahren, wie wir aus Erfahrungen wissen, wenn Menschen über einen längeren Zeitraum ohne Privatsphäre leben müssen.

Ich beschränke mich im Folgenden im Wesentlichen auf den Bundesnachrichtendienst (BND), soweit ich nicht ausdrücklich Militärischer Abschirmdienst (MAD) und Bundesamt für Verfassungsschutz (BfV) anspreche. Zunächst ein kurzer Blick in das BND-Gesetz: Aufgaben des BND sind das Sammeln von Nachrichten über das Ausland (§ 1 Abs. 2 BNDG). Hierzu hat der BND die Befugnis zur Erhebung, Verarbeitung und Nutzung der Informationen (§ 2 BNDG).

Zur Überwachung speziell der Telekommunikation ist im BND-Gesetz insoweit *nichts* geregelt. Von der neuen Regelung zum Auskunftsverlangen gegenüber Anbietern von Telekommunikationsdiensten oder Telediensten abgesehen, siehe z. B. § 2 a BND-Gesetz.

Im BND-Gesetz, gleiches gilt für BfV und MAD, gibt es also keine entsprechenden Befugnisse für umfassende Eingriffe in das Fernmeldegeheimnis bzw. für entsprechende „Beschränkungen".

DAS G-10-GESETZ

Ein solches Gesetz stellt aber das „Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses" dar, kurz „G-10-Gesetz" genannt. Nach dessen §§ 3 ff. dürfen die deutschen Nachrichtendienste unter den dort genannten Voraussetzungen „Beschränkungen in Einzelfällen" vornehmen, also etwa einzelne Fernmeldegespräche abhören.

Darum geht es aber hier nicht, sondern es interessiert, ob deutsche Nachrichtendienste eine ähnliche umfangreiche Überwachung, wie dies laut den Papieren von Edward Snowden NSA und GCHQ durchführen, vornehmen dürfen oder wo für den BND hier die rechtlichen Grenzen lägen.

Hierzu sagen Art. 5 und Art. 10 G-10-Gesetz, welche die sog. Strategische Fernmeldeüberwachung / Strategische Beschränkungen durch den BND regeln, folgendes: „Auf Antrag des Bundesnachrichtendienstes dürfen Beschränkungen nach § 1 (Überwachung und Aufzeichnung der Telekommunikation) für internationale Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt, angeordnet werden." (§ 5 Abs. 1 Satz 1 G 10-Gesetz)

Voraussetzungen sind danach:

- Es muss sich um internationale Telekommunikationsbeziehungen handeln, soweit eine Übertragung „gebündelt" erfolgt, also keine Einzelgespräche.
- Diese zu überwachenden internationalen Telekommunikationsbeziehungen werden nicht vom BND selbst, sondern vom Bundesministerium des Innern mit Zustimmung des Parlamentarischen Kontrollgremiums bestimmt. Dabei sind auch das Gebiet, über das Informationen gesammelt werden sollen, und die Übertragungswege zu benennen, die der Beschränkung / Überwachung unterliegen.
- Ziel ist, drohende schwerste Gefahren für Deutschland, wie etwa bewaffnete Angriffe, internationale terroristische Anschläge, internationale Verbreitung von Kriegswaffen, internationalen bandenmäßigen Rauschgifthandel usw., zu erkennen.
- Hierbei (§ 5 Abs. 2) ist nur die Suche mit zur speziellen Aufklärung bestimmten und geeigneten Suchbegriffen zulässig; diese dürfen

zudem nicht Merkmale enthalten, die gezielt bestimmte Telekommunikationsanschlüsse identifizieren, und diese dürfen nicht den Kernbereich privater Lebensgestaltung betreffen (was im Schlafzimmer geschieht). Die Suchbegriffe sind ebenfalls in der Anordnung des BMI zu benennen (§ 10 Abs. 4).

- § 5 Abs. 2 Satz 3: Nur Telefonanschlüsse im Ausland, deren Inhaber oder regelmäßige Nutzer nicht Deutsche sind, sind vom besonderen Schutz ausgenommen. Versehentlich erfasste Daten zu Deutschen werden unverzüglich gelöscht.
- Außerdem dürfen bei der strategischen Fernmeldekontrolle nur maximal 20 % der auf dem jeweiligen Übertragungsweg zur Verfügung stehenden Kapazität überwacht werden (§ 10 Abs. 4 Satz 4). Tatsächlich liegt der Anteil in der Regel wegen Grenzen der technischen Kapazitäten deutlich niedriger.
- Die G-10-Kommission ist vom Bundesministerium des Innern (BMI) grundsätzlich vor deren Vollzug über derartige beabsichtige Beschränkungsmaßnahmen zu unterrichten (§ 15 Abs. 6). Anordnungen, die die Kommission als unzulässig oder als nicht notwendig erklärt, muss das BMI unverzüglich aufheben. Diese dürfen also nicht durchgeführt werden.

Damit wird jedenfalls deutlich, dass eine flächendeckende, vollständige Überwachung des internationalen oder eines überwiegend ausländischen Telekommunikationsverkehrs durch den BND vom G-10-Gesetz nicht geregelt und damit jedenfalls auch *nicht gestattet* ist. Dass weitergehende Beschränkungen nicht geregelt sind, heißt nicht, dass diese ohne gesetzliche Regelung zulässig wären.

Übrigens hat das Bundesverfassungsgericht die in § 5 G-10-Gesetz geregelte strategische Telekommunikationsüberwachung durch den BND in seiner Entscheidung vom 14. Juli 1999 grundsätzlich als mit dem Grundgesetz vereinbar erklärt.[2] Die vom Bundesverfassungsgericht damals gemachten Monita (z. B. Unterrichtungspflichten) sind nachfolgend in das G-10-Gesetz eingearbeitet worden.

In dieser Entscheidung hat das Bundesverfassungsgericht einen Bezug zum Schutzbereich von Art. 10 GG bereits dann angenommen, wenn die Abhöranlagen, mit denen der internationale Fernmeldeverkehr aufgefangen wird, auf deutschem Boden stehen oder die empfangenen Telekommunikationsverkehre im Inland ausgewertet werden.

Wie stellt sich aber die Rechtslage dar, wenn der BND den Telekommunikationsverkehr außerhalb des im G-10-Gesetz geregelten Bereichs (etwa zusätzlich zur strategischen Telekommunikationsüberwachung) im Ausland überwacht? In Betracht kommen kann insoweit eine Überwachung der Telekommunikation z. B. in einem Einsatzland der Bundeswehr zu deren und etwaiger NATO-Partner Schutz oder die Überwachung von Funkverkehr oder sonstigem Telekommunikationsverkehr im sogenannten „offenen Himmel".

Gilt das Grundrecht des Art. 10 GG auch im Ausland und auch gegenüber Ausländern? In diesem Fall wäre eine entsprechende gesetzliche Regelung notwendig, welche die Überwachung dieser Telekommunikationsverkehre gestattet. Unabhängig davon wäre eine gesetzliche Regelung bereits dann erforderlich, wenn trotz Überwachung im Ausland der Bezug zum Inland durch die Verarbeitung der abgehörten Daten gegeben wäre.

Von Seiten der Bundesregierung wird ein besonderer Regelungsbedarf für eine Telekommunikationsüberwachung im Ausland offensichtlich nicht gesehen. Vor dem Bundesverfassungsgericht hatte die Bundesregierung im Zusammenhang mit der strategischen Telekommunikationsüberwachung vorgetragen, dass Fernmeldeverkehre von Ausländern im Ausland von Art. 10 GG nicht geschützt seien. Bei Ausländern im Ausland fehle der für den Grundrechtsschutz erforderliche territoriale Bezug.[3] Die Fernmeldeaufklärung im Ausland könne auf die Aufgabenzuweisung des § 1 Abs. 2 Satz 1 BNDG gestützt werden. Die reine Auslandsaufklärung des Fernmeldeverkehrs durch den BND unterfalle nicht Art. 10 GG. Ein Grundrechtseingriff – hier also in Art. 10 GG – setze eine die Schutzbedürftigkeit begründende Gebietsbezogenheit voraus.[4] Art. 10 GG unterfielen nur solche Telekommunikationsverkehre, die „von und nach Deutschland geführt" würden.[5]

In jüngster Zeit erheben sich jedoch ernstzunehmende Gegenstimmen: So hat das langjährige Mitglied der G-10-Kommission Huber 2013 mit einem Aufsatz in der größten deutschen juristischen Fachzeitschrift für große Aufmerksamkeit gesorgt, als er die Überwachung des Fernmeldeverkehrs im Ausland über das Ausland durch den BND als verfassungswidrig bezeichnet hat.[6] Ihm sind die Gutachter des NSA-Untersuchungsausschusses, die Professoren Bäcker, Hoffmann-Riem und bis zu einem gewissen Umfang auch Prof. Papier, letzterer als ehemaliger Präsident des Bundesverfassungsgerichts besonders prominent, grundsätzlich gefolgt. Damit ist die Debatte über die Rechtfertigung der über § 5 G-10-Gestz hinausgehenden Fernmeldeaufklärung des BND im Ausland eröffnet.

Was lässt sich zu dieser Frage aus den bisherigen Entscheidungen des Bundesverfassungsgerichts entnehmen? Ich zitiere insbesondere aus der Entscheidung vom 14. Juli 1999, die sich mit der strategischen Telekommunikationsüberwachung durch den BND befasst:[7]

„Wie weit der Schutz des Art. 10 GG in räumlicher Hinsicht reicht, ist in der Verfassungsrechtsprechung bisher nicht geklärt [...]. Ansatzpunkt für die Beantwortung der Frage nach der räumlichen Geltung von Art. 10 GG ist Art. 1 Abs. 3 GG, der den Geltungsumfang der Grundrechte im Allgemeinen bestimmt. Aus dem Umstand, dass diese Vorschrift eine umfassende Bindung von Gesetzgebung, vollziehender Gewalt und Rechtsprechung an die Grundrechte vorsieht, ergibt sich noch keine abschließende Festlegung der räumlichen Geltungsreichweite der Grundrechte. Das Grundgesetz [...] bestimmt auch in Grundzügen sein Verhältnis zur Staatengemeinschaft." [...] So „muss das Verfassungsrecht mit dem Völkerrecht abgestimmt werden". Das BVerfG führt hierzu dann aus:[8] „Der Schutz des Fernmeldegeheimnisses in Art. 10 GG zielt – im Einklang mit den völkerrechtlichen Bestimmungen[9] – darauf, dass die Fernmeldekommunikation von unerwünschter oder unbemerkter Überwachung frei bleibt." Diese völkerrechtlichen Bestimmungen binden übrigens auch die deutsche Staatsgewalt, gelten also auch grundsätzlich für den BND; hierzu noch später.

Eine präzise Antwort auf die Frage, was der BND im Rahmen der Telekommunikationsüberwachung außerhalb des vom G-10-Gesetz gezogenen Rahmens tun darf, gibt das BVerfG allerdings nicht.

Es sagt zwar in der genannten Entscheidung ausdrücklich:[10] „Über geheimdienstliche Tätigkeiten, die nicht dem G-10-Gesetz unterliegen, ist hier ebenso wenig zu entscheiden wie über die Frage, was für ausländische Kommunikationsteilnehmer im Ausland gilt." Andererseits führt es aus, dass „bereits durch die Erfassung und Aufzeichnung des Telekommunikationsverkehrs mit Hilfe der auf deutschem Boden stationierten Empfangsanlagen des Bundesnachrichtendienstes eine technisch-informationelle Beziehung zu den jeweiligen Kommunikationsteilnehmern [...] und ein Gebietskontakt hergestellt" wird. „Auch die Auswertung der so erfassten Telekommunikationsvorgänge durch den Bundesnachrichtendienst findet auf deutschem Boden statt." Daraus zieht das BVerfG im folgenden Satz den Schluss: „Unter diesen Umständen ist aber auch eine Kommunikation im Ausland mit staatlichem Handeln im Inland derart verknüpft, dass die Bindung durch Art. 10 GG selbst dann eingreift, wenn man dafür einen hinreichenden territorialen Bezug voraussetzen wollte."[11] Dieser Schluss wird verstärkt durch die Entscheidung des BVerfG zur Vorratsdatenverarbeitung vom 3. März 2010:[12] „In der Erfassung von Telekommunikationsdaten, ihrer Speicherung, ihrem Abgleich mit anderen Daten, ihrer Auswertung, ihrer Selektierung zur weiteren Verwendung oder ihrer Übermittlung an Dritte liegen damit je eigene Eingriffe in das Telekommunikationsgeheimnis."[13]

Damit bedeutet diese Aussage des Bundesverfassungsgerichts wohl, dass auch für das Überwachen des „offenen Himmels" Art. 10 GG jedenfalls dann gilt, wenn entweder deutsche Staatsangehörige betroffen sind oder außerdem unabhängig vom Standort der Überwachungseinrichtungen zumindest die Auswertung der erhobenen Daten im Inland erfolgt. Ist dies aber der Fall, bedarf es selbst für die Überwachungen des „offenen Himmels" einer (Art. 5 ff. G-10-Gesetz vergleichbarer) gesetzlicher Regelung.

Wird im Rahmen militärischer Einsätze die komplette Telekommunikationsüberwachung einschließlich deren Auswertung im Ausland durchgeführt, so wird, abgesehen von der immer zu schützenden Menschenwürde, das für diesen speziellen Einsatz geltende Recht (UN, NATO, internationale Konventionen, Völkerrecht) zu berücksichtigen sein.

Auf Einzelheiten, wie genau eine Regelung für die Überwachung der internationalen Telekommunikation (offener Himmel) beschaffen sein müsste, will ich nicht im Detail eingehen. Hierzu nur so viel:

- Bezüglich der exakten Tiefe einer solchen gesetzlichen Regelung kann ggf. auch der Satz des Bundesverfassungsgerichts in einer früheren Entscheidung[14] herangezogen werden, dass unter bestimmten Umständen „aber eine Minderung des Grundrechtsstandards in Kauf zu nehmen“ ist, wenn Eingriffe mit Auslandsbezug vorliegen. Diese Minderung mag etwa für reine Auslandsfälle gelten, soweit es um gesetzliche Erfordernisse bezüglich der Benachrichtigungen an Betroffene oder hinsichtlich der Überwachung militärischer Verkehre geht.
- Die Kernsätze des Grundgesetzes, also insbesondere die Grundrechte und der Maßstab der Verhältnismäßigkeit, sind in ihrem Kerngehalt aber immer zu beachten, wenn deutsche Behörden wo auch immer agieren. So könnten aus rein deutscher Sicht Anhaltspunkte für eine mögliche gesetzliche Regelung der Voraussetzungen für eine derartige Überwachung sowie der hierbei zu beachtenden Grenzen die Regelungen der Art. 5 ff. G-10-Gesetz sein.
- Sind Einschränkungen durch Völkerrecht und geschriebenes internationales Recht für Überwachungsaktivitäten deutscher Nachrichtendienste im Ausland bei einer entsprechenden deutschen gesetzlichen Regelung zu berücksichtigen?

Zum Völkerrecht: Allgemein gilt als anerkannt, dass das Völkerrecht Spionage nicht grundsätzlich verbietet. Wohl gemerkt, das Völkerrecht erlaubt Spionage nicht ausdrücklich, diese Annahme wiederum wäre nicht richtig, aber das Völkerrecht in seiner Anpassung an Realitäten nimmt Spionage hin. Allerdings – ohne dass dies im Einzelnen schon abschließend geklärt wäre – wird im Völkerrecht Spionage wohl vorrangig als gegen ausländisches Regierungshandeln und insbesondere zur Aufklärung ausländischer militärischer Aktivitäten gesehen. Bei der reinen Wirtschaftsspionage ohne Bezug zu militärischer Stärke des Auslands dürfte diese völkerrechtliche Akzeptanz nicht mehr so eindeutig sein. Neuere technische Entwicklungen, die auch den zivilen Telekommunikationsverkehr weitgehend vollständig erfassen können, sind völkerrechtlich wohl noch nicht näher „geprüft“.

Wo können aus europäischem und internationalem Recht gleichwohl Grenzen für Spionage ganz generell und damit der internationalen Telekommunikationsüberwachung entnommen werden? Nun, eine Grenze, die mit keinem staatlichen Akt überschritten werden darf, wo auch immer dieser ausgeführt wird, ist die Achtung der Menschenrechte, insbesondere der Menschenwürde. Dies ergibt sich eindeutig aus der UN-Charta, der Allgemeinen Erklärung der Menschenrechte sowie in Europa aus der Europäischen Menschenrechtskonvention. Daraus ergeben sich Schranken für eine Totalüberwachung auch ausländischer Bürger, insbesondere hinsichtlich deren Kernbereichs privater Lebensgestaltung. Das kann bei künftigen noch weitergehenden technischen Fähigkeiten, die vielleicht eine totale Überwachung der Bürger weltweit ermöglichen, eine Rolle spielen und diesen rechtliche Grenzen setzen. Insoweit erinnere ich an das o. a. Zitat des BVerfG bezüglich des internationalen Rechts in der G-10-Gesetz-Entscheidung.

Eine weitere Schranke für internationale Telekommunikationsüberwachung sollte sich aus internationalen, zwischenstaatlichen Vertragsbeziehungen ergeben. Hier gilt prinzipiell auch im internationalen Recht der Grundsatz der Beachtung des „Geistes“ eines Vertrages. Auf das Thema der Überwachung internationaler Telekommunikation umgemünzt bedeutet dies: Unter vertraglich Verbündeten spioniert man nicht. Dieser Grundsatz wäre in der EU etwa unter deren Mitgliedern zu beachten, wie dies auch innerhalb der NATO zu gelten hätte. Allerdings wird dieser Grundsatz oftmals nicht respektiert und hat somit in Folge im Völker-

recht eine nur eingeschränkte und jedenfalls nicht „einklagbare“ Bedeutung. Auch hier gilt faktisch leider das Recht des Stärkeren.

Zwischenergebnis: Für die Überwachung des offenen Himmels ist eine gesetzliche Regelung notwendig, wenn nicht ausschließlich Ausländer im Ausland betroffen sind und die Verarbeitung ebenfalls ausschließlich im Ausland erfolgt.

Warum sperrt sich die Bundesregierung gegen eine Ergänzung des G-10-Gesetzes, die ich als eine Art Minimallösung für erforderlich sehe? Nun die Antwort könnte in dem gleichen Grund liegen, weshalb überhaupt so spät, nämlich erst 1990, erstmals ein BND-Gesetzes erlassen worden war. Auch wenn völkerrechtlich die Spionage als nicht verboten gilt, ist es nicht unproblematisch, die Spionage im Ausland zu regeln. Wie aber etwa die §§ 5 ff. und § 8 (Leib und Leben einer Person im Ausland) des G-10-Gesetzes zeigen, ließe sich dieses Problem durch entsprechende Formulierungen aber lösen. Ich ziehe folgende Schlussfolgerung:

Aus alledem lässt sich jedenfalls der m. E. gut vertretbare Schluss ziehen, dass deutsche Behörden grundsätzlich, wo immer sie tätig werden, bei ihrem Handeln die Menschenrechte und die Grundrechte zu achten haben. Das gilt auch für den BND. Also jedenfalls immer dann, wenn der BND aus dem Ausland gewonnene Daten auswertet, hat er dies im Rahmen des Grundgesetzes unter Beachtung des Art. 10 GG zu tun. Dafür ist nach Art. 10 Abs. 2 GG aber eine ausdrückliche gesetzliche Erlaubnis erforderlich.

Bei einer ohnehin notwendigen Aktualisierung der Gesetze zu den deutschen Nachrichtendiensten ist auch der Aufgabenbereich der Überwachung der internationalen Telekommunikation im „offenen Himmel“ durch die Nachrichtendienste gesetzlich zu regeln. Die derzeitigen Gesetze bieten nach meiner Überzeugung hierfür keine ausreichende Rechtsgrundlage. Der BND braucht, gleiches gilt für die anderen deutschen Dienste, sofern neue Erfordernisse an die Überwachung der Telekommunikation gestellt werden, auch hier eine klare gesetzliche Basis und darf nicht von der Politik im juristischen Zwielicht gelassen werden.

Kritik wird auch an der geltenden Fassung der §§ 5 ff. G-10-Gesetz geübt: Der aktuelle, zuletzt am 6. Juni 2013 novellierte Gesetzestext ist vom Bundesverfassungsgericht zwischenzeitlich noch nicht erneut geprüft worden.

- Zu prüfen sei, ob die Befugnis zur strategischen Telekommunikationsüberwachung insbesondere im Licht der rasanten Zunahme der Datenmengen beim internationalen Telekommunikationsverkehr und der entsprechenden technischen Fortschritte präzisiert werden müsste.
- Verschiedentlich geäußerte Kritikpunkte sind hierbei etwa die mangelnde Schärfe der Formulierung zu der Begrenzung der Überwachung auf 20 % der jeweiligen Übertragungskapazität in § 10 Abs. 4 Satz 2 G-10-Gesetz.
- Kritisiert wird etwa auch, dass bei der Überwachung von Telekommunikationsanschlüssen von Ausländern, die zudem im Ausland liegen, die Verbote der Verwendung von solchen Suchbegriffen, die Identifizierungsmerkmale zur gezielten Erfassung von Anschlüssen enthalten oder die den „Kernbereich privater Lebensgestaltung“ betreffen, (§ 5 Abs. 2 Satz 3 G-10-Gesetz) ausdrücklich ausgenommen sind. Ich teile diese Kritik; die Menschenwürde ist gegenüber jedermann von deutschen Behörden zu achten.

Um nun hier keine gesetzlichen Lücken entstehen zu lassen, empfiehlt sich eine entsprechende Ergänzung des G-10-Gesetzes.

DIE HERAUSFORDERUNGEN IM DIGITALEN ZEITALTER IN DEUTSCHLAND UND IN EUROPA

Zunächst einmal ist folgendes zu konstatieren: Aus der Rechtsprechung des deutschen Bundesverfassungsgerichts und des Europäischen Gerichtshofs folgt eine Handlungsverpflichtung der jeweiligen Regierungen, um die aus der Digitalisierung entstehenden Risiken für die Bürger zumindest zu verringern, wenn diese schon nicht komplett zu verhindern sind.

Diese Handlungsverpflichtung des Staates gilt zum einen bezüglich der umfassenden Datenausspähung durch Nachrichtendienste und andere Sicherheitsbehörden. Für staatliche Stellen bedeutet dies, dass Eingriffe in die „Privatsphäre“ verhältnismäßig sein müssen. Dafür haben die verantwortlichen Regierungen zu sorgen.

Aber auch für die großen Internet-Firmen wie Google, Facebook, Microsoft, Yahoo u. a. darf es keinen rechtsfreien Raum geben. Der Handlungsverpflichtung des Staates gegenüber diesen Unternehmen steht auch nicht entgegen, dass scheinbar viele Bürger ihr Recht auf selbstbestimmtes Leben der Alltagsbequemlichkeit unterordnen, die ihnen von den Internet-Konzernen angeboten wird.

NOTWENDIGE MAßNAHMEN ZUM SCHUTZ DER PRIVATSPHÄRE DER BÜRGER

Hier muss zunächst einmal unterschieden werden zwischen

- Maßnahmen zum Schutz der Bürger gegen ein überbordendes Ausforschen durch innerstaatliche Stellen und durch ausländische staatliche Stellen, wie etwa durch ausländische Nachrichtendienste auf der einen Seite und
- den Aktivitäten privater Konzerne.

Beim Schutz gegen ausländische staatliche Stellen ist an folgende Maßnahmen zu denken:

- Das Routing des nationalen Mailverkehrs nur über nationale Telekommunikationsleitungen und das Abschirmen des europäischen E-Mail-Verkehrs schützt europäische Bürger. Mit einem „Internet der kurzen Wege“ wird verhindert, dass Datenverkehre mit Sender und Empfänger in Europa nicht über Amerika oder andere Kontinente geleitet werden. Gegen ein derartiges nationales Routing war bereits Protest aus den USA zu hören.[15]
- Durch das Meiden außereuropäischer Speicherdienste, also dem Cloud-Computing bei Anbietern, die die Server außerhalb Europas stehen haben, wird der unberechtigte Zugriff auf wichtige Datenbestände zumindest erschwert.
- Mit einem Intelligence-Kodex zwischen den Nachrichtendiensten innerhalb der EU und unter verbündeten Staaten müsste die gegenseitige Spionage untersagt werden.
- Der verstärkte Einsatz von Verschlüsselungssoftware würde die Auswertung der Telekommunikation durch Unbefugte erschweren. Allerdings ist dies kein wirksamer Schutz gegenüber einer Auswertung durch Internetfirmen, wenn deren Angebote genutzt werden, wie etwa die Suche bei Google.

Selbst die Rechtsprechung hat bereits wichtige Entscheidungen zum Schutz der Privatsphäre getroffen, die über den jeweiligen Einzelfall hinaus deutliche Hinweise für einen weitgehenden Schutz der Privatsphäre im digitalen Zeitalter geben. Wie eingangs bereits kurz erwähnt, hat insbesondere das deutsche Bundesverfassungsgericht maßgebliche Hinweise gegeben – wie etwa zur Rasterfahndung oder zum deutschen Gesetz zur Vorratsdatenspeicherung. Maßgeblich ist danach immer, die richtige Balance zwischen Freiheit und Sicherheit zu finden. Auch bei der Abwehr schwerer Gefahren für die öffentliche Sicherheit müssen Eingriffe in die Privatsphäre der Bürger verhältnismäßig sein. Auf europäischer Ebene geht die Entscheidung des Europäischen Gerichtshofes vom 8. April 2014 in die gleiche Richtung, welche die Richtlinie zur Vorratsdatenspeicherung für ungültig erklärt. Diese Entscheidungen müssen bei der Gesetzgebung berücksichtigt werden.

Schließlich müssen die Gesetze zur Überwachung der Telekommunikation und zu den Telemediendiensten wie Twitter, Facebook und andere aufeinander abgestimmt werden. Die Kommunikation der Bürger ist nicht mehr nur auf die „alten“ Telekommunikationsmedien begrenzt.

Weitere Forderungen zum Schutz der Privatsphäre gegenüber den großen Internet-Konzernen:

Es sind neue und weitergehende Gesetze zum Schutz der Privatsphäre erforderlich, hierzu brauchen wir zum Beispiel einen gesetzlich gesicherten „Verbraucherschutz“ im Internet. Der Einzelne ist mit den Abläufen im Internet oft überfordert. Er kann die Wirkungen seiner Aktivitäten im Internet nicht immer übersehen. Er schließt manchmal einen Vertrag über kostenträchtige digitale Dienstleistungen, ohne sich dessen vollständig bewusst zu sein, oder akzeptiert versehentlich für ihn nachteilige Vertragsbedingungen usw. Hier muss der Staat zum Schutz der Bürger helfend eingreifen.

Deshalb muss eine „Verbraucherschutz“-Gesetzgebung für die digitale Welt den Einzelnen vor Gefährdungen schützen. Dazu gehören beispielsweise klare Regelungen, dass Daten über Einzelne nur nach deren ausdrücklichen Einwilligung ausgewertet und gespeichert wer-

den dürfen. Vorab ist der Einzelne über die Folgen einer solchen Einwilligung genau aufzuklären („informed consent"). Weiter muss geregelt werden, dass große Internet-Unternehmen nicht ihre marktbeherrschende Stellung dazu missbrauchen, vom Einzelnen faktisch die Einwilligung in eine unverhältnismäßige Nutzung der Daten zu erzwingen, weil er andernfalls von der in der Gesellschaft üblich gewordenen Kommunikation und der Nutzung der Informationstechnologien ausgeschlossen wäre.

Am besten wären insoweit Regelungen auf europäischer Ebene, um nicht nur in einem einzelnen Staat Wirkung zu erzielen.

Solche den Verbraucher / Bürger schützende Gesetze könnten übrigens auch Gegenstand bei den derzeit geführten Verhandlungen zwischen der Europäischen Union und den USA zu einem neuen Handelsabkommen (TTIP) werden. Dann würde auch klar, ob etwa die USA bereit sind, europäische Standards zum Schutz der Privatsphäre zu akzeptieren.

Recht auf Vergessen

Computer „vergessen" nichts, wenn nicht die Löschung von Daten ausdrücklich angeordnet wird. Wir Menschen haben aber grundsätzlich das Recht, dass nachteilige Dinge uns nicht ein Leben lang entgegengehalten werden. Das menschliche Gehirn, das durchaus vergisst, hilft uns hierbei. Umso mehr und umso detailliertere Daten über die einzelnen Menschen über die großen Suchmaschinen auf Dauer zur Verfügung gestellt werden, umso wichtiger wird auch eine Regelung, die eine zeitliche Schranke für das Bereitstellen von Daten setzt.

Ein solches „Recht auf Vergessen" sollte in zweierlei Weise wirken. Zum einen sollte es gelten hinsichtlich solcher Informationen, die von Dritten etwa über Webseiten im Internet eingestellt sind, wenn dadurch Persönlichkeitsrechte tangiert werden. Inzwischen gibt es zur Frage der Löschung von Daten schon eine aktuelle Entscheidung des Europäischen Gerichtshofs vom 12. Mai 2014. Darin fordert das Gericht, dass Google unter bestimmten Voraussetzungen zumindest die Links zu Seiten mit nachteiligen Inhalten löscht.

Über die interessante Frage der Unterbrechung der Links zu Webseiten hinaus enthält diese Entscheidung des Europäischen Gerichtshofs einige wichtige Aussagen zur Datenverarbeitung und zum Schutz der Bürger im digitalen Zeitalter:

Auch der Betreiber einer Suchmaschine, der selbst keine Daten speichert, sondern „nur" das Internet automatisch und systematisch auf die dort gespeicherten Informationen durchforstet und dann in Form von Ergebnislisten an seine Nutzer weitergibt, betreibt „Datenverarbeitung" mit personenbezogenen Daten und ist eine im Sinne der Normen zum Schutz der Privatsphäre „verantwortliche Stelle". Selbst „durch die Tätigkeit einer Suchmaschine können die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten erheblich beeinträchtigt werden." Mit der Ergebnisliste ermöglicht der Betreiber der Suchmaschine einen strukturierten Überblick über die zu der betreffenden Person im Internet zu findenden Informationen, die potenziell zahlreiche Aspekte von deren Privatleben betreffen. Der Betreiber von Suchmaschinen kann sich deshalb den einschlägigen gesetzlichen Verpflichtungen zum Datenschutz nicht entziehen.

Auch ein Betreiber von Suchmaschinen mit Sitz in den USA, also außerhalb Europas, ist europäischen Gesetzen unterworfen, wenn er eine Tochtergesellschaft zur Förderung seiner Aktivitäten in einem europäischen Land hat.

Google ist zumindest in Europa verpflichtet, von der Ergebnisliste, die aus einer Recherche nach dem Namen einer bestimmten Person entstanden ist, Links zu von Dritten über diese Person veröffentlichte Internet-Seiten zu entfernen. Dabei spielt es eine Rolle, ob die Informationen zu dieser Person schon lange zurückliegen und ob die Informationen diese Person unnötig belasten, weil der der Speicherung zugrundeliegende Sachverhalt sich erledigt hat.

Allerdings ist auch ein gegebenenfalls anerkanntes Interesse der Öffentlichkeit an diesen Informationen zu berücksichtigen. Dies kann beispielsweise der Fall sein, wenn die betroffene Person, etwa wegen ihrer herausgehobenen Stellung, im besonderen Licht der Öffentlichkeit steht. Diese Abwägung zwischen Schutz der Privatsphäre und Meinungsfreiheit ist im Einzelfall zu treffen.

Ein weiterer Aspekt beim Recht auf Vergessen: Das Recht auf Löschen von Daten und damit das Recht auf Vergessen sollte darüber hinaus auch für von Betroffenen selbst in das Netz eingestellte Daten erwogen werden:

Auch wer beispielsweise als Jugendlicher leichtsinnig selbst Daten in Netzwerke wie Facebook und ähnliche eingestellt hat, muss das durchsetzbare Recht erhalten, diese Daten grundsätzlich wieder löschen zu können. Wer Daten in soziale Netzwerke einstellt, darf nicht dadurch, dass „Computer nichts vergessen", das Recht über diese seine Daten ein Leben lang verlieren. Der Einzelne muss Herr seiner Daten bleiben können. Dazu gehört eben auch das Recht, früher Geschriebenes nach noch festzulegenden Regeln aus dem Netz zu entfernen.

Kontrollen

Schließlich müssen wirksame Kontrollen sicherstellen, dass die Rechte der Bürger im Internet auch tatsächlich gewahrt werden.

Diesen Kontrollen müssen die Internet-Firmen unterworfen werden. Wegen deren internationalen Aktivitäten wäre hier auch ein international abgestimmtes Vorgehen angemessen. Solange eine solche gemeinsame und abgestimmte Kontrolle nicht erreicht wird, müssen die Nationalstaaten dafür Sorge tragen, dass die auf ihrem Hoheitsgebiet tätigen Internet-Firmen sich zumindest insoweit der Kontrolle unterwerfen.

Selbstverständlich müssen auch die staatlichen Akteure hinsichtlich ihrer Aktivitäten im Internet kontrolliert werden. Dies gilt besonders für die Nachrichtendienste und andere Sicherheitsbehörden wie etwa die Polizei.

In Deutschland stehen diese Forderungen nicht im rechtsfreien Raum. Vielmehr ergibt sich für den Staat aus dem Grundrecht auf „Schutz der Vertraulichkeit und der Integrität informationstechnischer Systeme" die Pflicht, die dafür notwendigen technisch-organisatorischen Sicherungsmaßnahmen zu ergreifen oder zumindest verpflichtend anzuordnen.

ZUSAMMENFASSUNG

Datenaskese, also das vollständige Ausklinken aus der Nutzung der neuen digitalen Technologien, kann nicht die Antwort auf deren Herausforderungen und Risiken sein. Das würde einen vollständigen Rückzug aus dem normalen Leben bedeuten, denn die Nutzung der digitalen Medien ist im Alltag heute unvermeidlich.

Aber aus den Verpflichtungen des deutschen Grundgesetzes zum Schutz der Grundrechte der Bürger und der europäischen Charta der Grundrechte ergibt sich ein Handlungszwang für die Politik, genauer für den Gesetzgeber, ein digitales Grundrecht und ein digitales Zivilrecht zu schaffen, das dem Einzelnen auch im digitalen Zeitalter erlaubt, als selbstbestimmtes Individuum und nicht als gesteuertes Objekt zu leben.

Der Bürger muss auch im digitalen Zeitalter Herr seiner „digitalen Souveränität" bleiben.

PROF. DR. HANSJÖRG GEIGER

Präsident des Bundesnachrichtendienstes a.D., Staatssekretär a.D., Berlin

ANMERKUNGEN

1 Urteil des Bundesverfassungsgerichts vom 24.3.2013, BVerfGE 133, 277/372 (Antiterrordatei).

2 Urteil des Bundesverfassungsgerichts vom 14.7.1999, BVerfGE 100, 313 ff. (Telekommunikationsüberwachung).

3 Bundesregierung, zitiert in BVerfGE 100, 313/338 f.

4 Zitiert ebd.

5 Vgl. auch die Gesetzesbegründung zur Novellierung des G 10, BT-Drs. 14/5655, S. 18; wohl ähnlich in Stellungnahmen zu parlamentarischen Anfragen während der 17. Wahlperiode; vgl. hierzu Hinweise bei Bäcker in seinem Gutachten für den U-Ausschuss, S. 17, FN. 58.

6 Huber, Bertold: Die Strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 ff.

7 BVerfGE 100, 313/362 f.

8 BVerfGE 100, 363.

9 Vgl. Art. 12 der Allgemeinen Erklärung der Menschenrechte vom 10. Dezember 1948; Art. 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten vom 4. November 1950.

[10] BVerfGE 100, 313/364.

[11] BVerfGE 100, 363 f.

[12] Urteil des Bundesverfassungsgerichts vom 3.3.2010, BVerfGE 125, 260/310 (Vorratsdatenverarbeitung).

[13] Vgl. BVerfGE 100, 313/366 f.

[14] Urteil des Bundesverfassungsgerichts vom 10.1.1995, BVerfGE 92, 26/42.

[15] Vgl. Welt, 15.4.2014.