BUCERIUS LAW SCHOOL
HOCHSCHULE FÜR RECHTSWISSENSCHAFT

Prof. Dr. W. Hoffmann-Riem, Jungiusstraße 6, 20355 Hamburg

Prof. Dr. Sensburg, MdB
NSA-Untersuchungsausschuss
Platz der Republik
11011 Berlin

Prof. Dr. Wolfgang Hoffmann-Riem
Richter des Bundesverfassungsgerichts a.D.
Friedrich-Stiftungsprofessur für rechtswissenschaftliche Innovationsforschung

Tel.: +49(0)40 6422 5848

wolfgang.hoffmann-riem@law-school.de

16. Mai 2014

Sachverständigengutachten

Sehr geehrter Herr Professor Sensburg,

nach Absendung meiner Stellungnahme.- die ich gern fristgerecht hatte vornehmen wollen – sind mir nicht nur Schreibfehler, sondern auch missverständliche Formulierungen aufgefallen. Deshalb habe ich eine korrigierte und z.T. leicht ergänzte Fassung gefertigt, die ich hiermit übersende. Ich bitte darum, diese Fassung an diejenigen zu verteilen, die schon die erste Fassung erhalten haben.

Mit freundlichen Grüßen
Ihr W. Hoffmann-Riem

BUCERIUS LAW SCHOOL
HOCHSCHULE FÜR RECHTSWISSENSCHAFT

Prof. Dr. Wolfgang Hoffmann-Riem
Richter des Bundesverfassungsgerichts a.D.
Friedrich-Stiftungsprofessur für rechts-
wissenschaftliche Innovationsforschung

Jungiusstraße 6
20355 Hamburg

16. Mai.2014

(mit Ergänzungen zu der Erstfassung vom 15. Mai 2014)

Stellungnahme
zur Anhörung des NSA-Untersuchungsausschusses
am 22. Mai 2014

Diese Stellungnahme[1] befasst sich mit Grundsatzfragen eines rechtlichen Schutzes vor Ausspähaktionen durch Zugriff auf Kommunikation in den globalen Kommunikationsinfrastrukturen (s. insbes. B IIII des Einsetzungsauftrags). Neben Ausführungen zur aktuellen Rechtslage, insbesondere den verfassungsrechtlichen Vorgaben, enthält sie insbesondere Überlegungen zu Schutzaufträgen und -pflichten im nationalen, unionalen und völkerrechtlichen Rechtsraum. Dabei geht sie - zumal es dazu auch Ausarbeitungen anderer, so des Wissenschaftlichen Dienstes, gibt und andere Sachverständige dort vermutlich Schwerpunkte setzen werden - nur zum Teil auf die vielen schriftlich

[1] Sie beruht teilweise auf meinem Aufsatz "Freiheitsschutz in den globalen Kommunikationsinfrastrukturen", in: JuristenZeitung 2014, S. 53 ff, geht aber thematisch darüber hinaus.

übermittelten Einzelfragen zur „Rechtslage nationales Recht“ (Anhörung 2) ein. Zu Antworten auf nicht behandelte Einzelfragen bin ich gerne in der mündlichen Anhörung bereit.

Inhaltsverzeichnis

A. Vorbemerkung

Die vom NSA-Untersuchungsausschuss zu bearbeitenden Fragen betreffen Eingriffe in Freiheitsrechte innerhalb und außerhalb Deutschlands. Rechtsschutz gegen Eingriffe im Territorialbereich Deutschlands kann zweifellos auf deutsches Recht gestützt - wenn auch vielfach aus praktischen Gründen nicht realisiert - werden. Rechtsschutz unter Einschluss von Grundrechtsschutz entfällt nicht allein schon wegen der Auslandsberührung eines Kommunikationsvorgangs oder der Durchführung eines Eingriffs in Kommunikationsvorgänge außerhalb Deutschlands.

Angesichts der Realität heutiger Kommunikationsvorgänge bei der Nutzung von IuK-Infrastrukturen wird ein Denken vorrangig in Kategorien räumlicher Verortung des Eingriffs oder des Aufenthalts betroffener Personen und Unternehmen den tatsächlichen Bedingungen der Gefährdung internationaler/globaler Kommunikationsinfrastrukturen und dem Schutzbedarf allerdings grundsätzlich nicht (mehr) gerecht. Die global organisierte Realität wäre sonst geeignet, den Freiheitsschutz weitgehend auszuhebeln. Deshalb bedarf es auch neuer Ansätze für rechtlichen Schutz.

Das Bundesverfassungsgericht hat vielfach anerkannt, dass die Änderung tatsächlicher Umstände Anlass sein kann und muss, die Grundrechte so auszulegen, dass das Niveau des Grundrechtschutzes erhalten bleibt.

Der Freiheitsschutz ist im vorliegenden Zusammenhang in erster Linie als Schutz der Kommunikationsinhalte und der mit der Übermittlung verbundenen Daten bedeutsam, aber auch als Schutz der für die Kommunikation genutzten Infrastrukturen, mit deren Hilfe die realen Voraussetzungen von Kommunikation und damit auch des Schutzes der Kommunikationsfreiheiten geschaffen werden. Auf diese verschiedenen Bezugspunkte muss der Schutz durch Grundrechte vorrangig bezogen werden. Die Frage, wo Eingriffe stattfinden und wer sie durchführt, verweist auf die weitere, die Frage nach dem Schutz des Inhalts und seiner Verbreitung nicht erübrigende Problematik, wo und wie Eingriffe abgewehrt werden können. Dabei stellen sich höchst unterschiedliche Rechtsfragen, darunter auch solche, deren befriedigende Beantwortung weitere gesetzliche und internationale Aktivitäten erfordert. Meine Ausführungen wollen auch Anregungen vermitteln, in welcher Hinsicht Lösungsmöglichkeiten gegeben sein können.

B. Anknüpfungspunkte für Grundrechtsschutz nach deutschem Verfassungsrecht

Im Folgenden seien die wichtigsten möglicherweise von Eingriffen betroffenen Grundrechte inhaltlich vorgestellt.

I. Grundrecht der Telekommunikationsfreiheit

Zu den maßgebenden Schutznormen gehört die Telekommunikationsfreiheit des Art. 10 GG. Sie ist Prüfungsmaßstab insoweit, als die Inhalte und Umstände der laufenden Telekommunikation im Telekommunikationsnetz erhoben, gespeichert sowie anschließend ausgewertet werden. Der Grundrechtsschutz gilt der Abwehr von solchen spezifischen Gefahren für die Kommunikation, die durch deren mit dem technischen Übermittlungsvorgang verbundene räumliche Distanz ermöglicht werden können.[2] Angesichts der realen Veränderungen im Telekommunikationssektor erstreckt das Gericht den Schutz auf Gefährdungen der Vertraulichkeit von Mitteilungen, die etwa durch die Vernetzung moderner Infrastrukturen der Telekommunikation und der Einschaltung mehrerer Dienste, auch fremder Übermittler, für einen Übermittlungsvorgang entstehen können.[3] Der Grundrechtsgehalt passt sich insoweit den technologischen Möglichkeiten im Aufbau der Infrastrukturen und den damit ermöglichten Arten der Dienste an. Thematisch bleibt der Schutz gleichwohl auf Gefährdungen während des konkreten Kommunikationsvorgangs beschränkt, erfasst also grundsätzlich nicht davon abgelöste Eingriffe am Endgerät oder Manipulationen der Hard- und Software der informationstechnischen Systeme.

II. Unverletzlichkeit der Wohnung

Erfolgt der Eingriff in Kommunikation demgegenüber in der räumlichen geschützten Sphäre, die durch das Wohnungsgrundrecht des Art. 13 GG geschützt ist, so bildet dieses den verfassungsrechtlichen Maßstab, etwa gegenüber der akustischen und optischen Wohnraumüberwachung, auch der Überwachung von außerhalb der Wohnung durch die

[2] Vgl. BVerfGE 106, 28, 36; 107, 299, 313. S. auch BVerfGE 125, 260, 309 ff.
[3] BVerfGE 85, 386, 396; 106, 28, 36.

Messung solcher elektromagnetischer Abstrahlungen[4], die mit der Nutzung informationstechnischer Systeme verbunden sind.[5]

III. Allgemeines Persönlichkeitsrecht

Das Allgemeine Persönlichkeitsrecht ist eine Fortführung der Garantie der freien Entfaltung der Persönlichkeit Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG). [6] Es umfasst mehrere Teilrechte, wie das Recht am gesprochenen Wort, am Bild u.a.

IV. Grundrecht auf informationelle Selbstbestimmung

Das Grundrecht auf informationelle Selbstbestimmung ist eine Weiterentwicklung des allgemeinen Persönlichkeitsrechts. Diese erfolgte im Anschluss an die politisch höchst umstrittene und heiß diskutierte Volkszählung. Die Entscheidung erging 1983[7], also ein Jahr vor 1984, das *George Orwell* als Titel seines futuristischen Romans über den „Big Brother" genutzt hatte. Das Bundesverfassungsgericht reagierte auf das Besorgnispotential mit einer Grundsatzentscheidung. Es schrieb u. a.: „Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen[8]."

Diese neue Grundrechtsverbürgung wurde die Grundlage des modernen Datenschutzrechts in Deutschland, insbesondere der allgemeinen Datenschutzgesetze sowie vieler Spezialregelungen über den Datenschutz und entsprechender Rechtsprechung. Deutschland wurde mit seiner Gesetzgebung - darunter dem Bundesdatenschutzgesetz - zum Vorreiter des Datenschutzes in mehreren Ländern.

---

[4] Nicht vom Schutz des Art. 13 GG erfasst sind allerdings mobil genutzte informationstechnische Systeme wie Laptop oder Mobiltelefone, wenn sie infiltriert werden, ohne dass durch den Eingriff die durch die Wohnung vermittelte räumliche Privatsphäre berührt wird, also insbesondere, ohne die Wohnung zu betreten, siehe BVerfGE 120, 274, 310 f.
[5] Vgl. BVerfGE 109, 279, 309, 327; 120, 274, 311.
[6] Siehe etwa BVerfGE 34, 238, 245 f.
[7] BVerfGE 65, 1.
[8] So lautet Leitsatz 1 in BVerfGE 65, 1; näher S. 41 ff.

Der gewählte Begriff „Grundrecht auf informationelle Selbstbestimmung“ allerdings erwies sich angesichts der weiteren Entwicklungen als zu eng. Die zunehmende Erosion der Möglichkeit autonomer Entscheidung prägt den Umgang mit den Informations- und Kommunikationsnetzen anvertrauten Daten und den mit ihnen transportierten Sinngehalten.

V. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

So erwies sich einige Jahre nach dem Volkszählungsurteil, dass dieser Schutz nicht weit genug reichte. Anlass waren Herausforderungen, auch Schutz gegen neuartige Eingriffe zu gewähren, die aufgrund neuer technologischer Entwicklungen möglich wurden. Die Überwachungsbehörden entwickelten neue Überwachungsmöglichkeiten, so in Gestalt der sogenannten Online-Durchsuchung. Diese ermöglicht eine Erfassung der Kommunikation am Endgerät, also einer „Kommunikation an der Quelle“/„Quellen-Telekommunikationsüberwachung“. Sie wurde zu der Zeit eingeführt, als die Überwachung der laufenden Kommunikation in Glasfasernetzen aus technischen Gründen (noch) praktisch ausschied.

Technisch erfolgt bei der Online-Durchsuchung eine Infiltration des vom Kommunikationsteilnehmer genutzten Computers durch bestimmte (Schad-)Software, sogenannte Trojaner, die es ermöglichen, die in dem System enthaltenen Funktions- und Inhaltsdaten heimlich zu erfassen und auszuwerten oder auch die Systeme zu manipulieren, etwa um den späteren leichteren Zugriff zu ermöglichen oder gar Fehlvorgänge zu initiieren. Während frühere Maßnahmen der Datenerhebung den Nutzern noch gewisse Selbstschutzmöglichkeiten der Abwehr einräumten, entfielen diese bei der Online-Durchsuchung regelmäßig. Die staatliche Infiltration sollte ja dazu dienen, mögliche Maßnahmen des Selbstschutzes der Bürger zu unterlaufen[9], also Maßnahmen, zu denen das Datenschutzrecht als Autonomieschutzrecht grundsätzlich ermuntern will. Der im Internet ohnehin gegebene weitgehende Verlust der Möglichkeit der autonomen Disposition über die weitere Verwendung der bei der Kommunikation anfallenden Daten aus dem eigenen Bereich und der Abbau der Möglichkeit von Kontrolle werden also durch den Zugriff am Endgerät vertieft. Es entstehen zugleich Risiken der Manipulation am informationstechnischen System,

[9] Vgl. auch die Feststellungen in BVerfGE 120, 274, 324.

die dessen Funktionsfähigkeit beeinträchtigen und Missbrauch, auch durch Dritte, ermöglichen können.

Aus Anlass einer Verfassungsbeschwerde, die sich gegen ein Gesetz wandte, das die Online-Durchsuchung legalisieren wollte, hat das Gericht festgestellt, dass die empirischen Prämissen des tradierten Grundrechtsschutzes sich verändert hätten. Es muss daher gesichert werden, dass die mit den Grundrechten in ihrem bisherigen Verständnis verbundenen normativen Prämissen - insbesondere das Ziel des freiheitssichernden Autonomieschutzes - auch angesichts der neuen technologischen Möglichkeiten bedeutsam bleiben, also angemessen verwirklicht werden können. Das Gericht ging in gleicher Weise wie früher vor, als es aus dem Grundrecht aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG die - im Grundgesetz nicht erwähnten, aber nach Auffassung des Gerichts von seinem Sinn erfassten - Rechte am eigenen Bild, am eigenen Wort sowie auf informationelle Selbstbestimmung als Konkretisierungen des allgemeinen Persönlichkeitsrechts ableitete. Es formulierte[10]: „Soweit kein hinreichender Schutz vor Persönlichkeitsgefährdungen besteht, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist, trägt das allgemeine Persönlichkeitsrecht dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet."

Dabei nahm das Gericht an, dass ein punktueller Schutz einzelner Kommunikationsvorgänge, wie ihn das Recht auf informationelle Selbstbestimmung ermöglicht, nicht mehr ausreicht, wenn der Eingriff das informationstechnische System insgesamt erfasst und manipuliert, und das schon bevor ein bestimmter Kommunikationsvorgang erfolgt oder nachdem die Kommunikation beim Empfänger angekommen ist. Individualschutz ist dann nicht mehr als Schutz des Kommunikationsvorgangs, sondern (wenn überhaupt) nur als Schutz des für die Absendung oder Speicherung genutzten informationstechnischen Systems effektiv möglich.[11] Ein solcher das System betreffender Schutz ist notwendig Vorsorge-Schutz. Insofern liegt die Entwicklung der neuen Grundrechtskonkretisierung in der Linie des Ausbaus von Grundrechtsvorsorge als Gegenüber der staatlichen Gefahren- und Strafverfolgungsvorsorge, dem ein Teil der staatlichen Überwachungsmaßnahmen dienen.

[10] BVerfGE 120, 274, 313.
[11] Dies verkennen die Kritiker der Entscheidung, die meinen, das überkommene Grundrecht auf informationelle Selbstbestimmung hätte ausgereicht.

Das Bundesverfassungsgericht hat damit ein seit langem anerkanntes Grundrecht, das allgemeine Persönlichkeitsrecht, angesichts neuer technologischer und gesellschaftlicher Entwicklungen durch eine weitere Ausdifferenzierung neuartig konkretisiert und zugleich mit einem die neue Schutzdimension kennzeichnenden Namen versehen, der zugleich verdeutlicht, dass Grundrechtsschutz auch die Gestalt von Systemschutz annehmen kann oder gar muss.

Durch die Umschreibung des grundrechtlichen Gewährleistungsauftrags als Schutz der „Vertraulichkeit und Integrität“ eigener (besser: eigen genutzter) informationstechnischer Systeme wurden Fragen der Funktionsfähigkeit solcher Systeme angesprochen: So in technologischer Hinsicht, etwa durch den Verweis darauf, dass die Installation eines „Trojaners“ auch von weiteren Personen (Dritten) zur Ausspähung genutzt werden könne.[12] Auch kann dies zu technischen Fehlfunktionen des informationstechnischen Systems führen. Die Begriffe „Vertraulichkeit und Integrität“ verweisen zusätzlich zur technologischen auch auf die soziale Funktionsfähigkeit: Die Bürger sollen grundsätzlich darauf vertrauen dürfen, dass die informationstechnischen Systeme nicht manipuliert werden und dass Kommunikation vertraulich bleibt.

Die neue Grundrechtskonkretisierung wird manchmal auch als „IT-Grundrecht“ oder „Computer-Grundrecht“ bezeichnet.

C. Zur Notwendigkeit der Anpassung des Freiheitsschutzes an Änderungen in der Kommunikationsrealität

Den neu bekannt gewordenen Gefährdungen kann zum Teil mit den geschilderten Freiheitsgewährleistungen begegnet werden. Es besteht aber auch ein Bedarf für Neuorientierungen.

Eingriffe in Kommunikationsvorgänge, auch solche zwischen Teilnehmern in Deutschland, sind nicht zwingend auf ein Handeln im Territorialbereich Deutschlands angewiesen. Da es (jedenfalls) für die übliche Kommunikation mit Hilfe der IuK-Infrastrukturen keine national abgegrenzten physischen Leitungen gibt[13], müssen die internationalen (regelmäßig globalen) Kommunikationsnetze mitgenutzt werden. Die über sie verbreiteten Daten werden regelmäßig unter Nutzung von Software versandt, die es ermöglicht, je nach Datenanfall und

[12] Siehe BVerfGE 120, 274, 314.
[13] Begrenzte Ausnahmen gibt es in Deutschland zum Beispiel für Kommunikation zwischen Behörden.

Kostengünstigkeit unterschiedliche Wege zu wählen. Ob bei dem Transportvorgang nur Knotenpunkte in Deutschland passiert werden, steht nicht von vornherein fest und ist jedenfalls für den Nutzer nicht vorhersehbar.

Insofern haben sich die empirischen Grundlagen von Kommunikation gegenüber früheren Zeiten verändert. Das hier vorrangig betroffene Fernmelde-/Telekommunikationsgeheimnis ist seinerzeit in Anlehnung an das Postgeheimnis entwickelt worden. Für beide war der territoriale Bezug sowohl bei der Bestimmung des Schutzbereichs als auch bei der Prüfung eines Eingriffs naheliegend. Die Beförderung von Briefen oder Paketen sowie die Nutzung physischer Telekommunikationsleitungen waren territorial gebunden. Transportmöglichkeiten auf dem Luftweg bildeten zwar Ausnahmen, schufen aber offensichtlich keinen Bedarf für andere Betrachtungen, da die Absende- und Empfangsorte territorial gebunden waren und zur rechtlichen Anknüpfung ausreichend erschienen.

Rechtsstaatlicher Freiheitsschutz gilt dem Kommunikationsvorgang selbst. Der Schutz würde teilweise leerlaufen, wenn er davon abhinge, ob ein Kommunikationsvorgang mehr oder minder unvorhersehbar/zufällig über Leitungen in deutschen oder in nichtdeutschen Gebieten abgewickelt wird. Es ist anerkannt, dass der Schutz durch die Grundrechte für jeden Grundrechtsträger gegen Eingriffe der deutschen Staatsgewalt besteht: „Die Grundrechte binden in ihrem sachlichen Geltungsumfang die deutsche öffentliche Gewalt auch, soweit Wirkungen ihrer Betätigung außerhalb des Hoheitsbereichs der Bundesrepublik Deutschland eintreten.“[14] Gleiches gilt, wenn deutsche Stellen einen Eingriff in Grundrechte außerhalb des deutschen Territoriums vornehmen.

Grundrechtsschutz als Schutz der Entfaltungsfreiheit knüpft an das Verhalten von Grundrechtsträgern an. Danach - und nicht nach den Zufälligkeiten eines, insbesondere eines von Dritten ohne Einwirkung der Kommunikatoren bestimmten, Transportwegs - richtet sich die Reichweite des Schutzes durch Kommunikations- und Persönlichkeitsgrundrechte. Dies bedeutet: Wer für seine grundrechtlich geschützte Kommunikation die internationalen/globalen Kommunikationsinfrastrukturen nutzt, ist genauso schutzwürdig und -bedürftig wie jemand, dessen Kommunikation über rein lokale Kommunikationswege erfolgt. Deshalb greift der Grundrechtsschutz auch, falls deutsche Hoheitsträger sich Zugang zu der Kommunikation außerhalb Deutschlands verschaffen.

[14] So BVerfGE 57, 9, 23 unter Berufung auf BVerfGE 6, 290, 295. Siehe auch *Kment*, Grenzüberschreitendes Verwaltungshandeln, 2010, S. 183; Siehe ferner *Yousif*, Die extraterritoriale Geltung der Grundrechte bei der Ausübung deutscher Staatsgewalt im Ausland (2007), S. 70 ff.

Ein Zugriff auf Metadaten und/oder auf die Inhalte der Kommunikation durch deutsche Hoheitsträger ist - einerlei wo er erfolgt - ein Grundrechtseingriff durch Realakt. Gegen ihn ist Grundrechtsschutz (s.o. B) gewährt Er ist nicht auf Deutsche begrenzt, da die die Kommunikationsfreiheit und die Persönlichkeitsrechte schützenden Grundrechte keine sog. Deutschenrechte sind.

D. Rechtliche Grenzen für Eingriffe durch deutsche Stellen - am Beispiel des Bundesnachrichtendienstes

I. Rechtliche Grenzen für Spähaktionen

Eingriffe in den Kommunikationsverkehr gehen auch von deutschen Stellen aus. Soweit diese - dies sei hier am Beispiel des Bundesnachrichtendienstes behandelt[15] - gesetzlich zu Eingriffen berechtigt sind, stellt das für sie maßgebende Recht - hier das BND-Gesetz -Anforderungen an die Datenerhebung und -verwendung. Ziel darf nach § 1 Abs. 2 Satz 1 BNDG nur die Gewinnung von Erkenntnissen über das Ausland sein, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. Das Gesetz normiert in § 1 - auch ausweislich der Überschrift - eine (bloße) Aufgabenumschreibung, keine Ermächtigung zu Grundrechtseingriffen zwecks Auslandsaufklärung. § 1 Abs. 2 Satz 1 BNDG verweist darüber hinaus auf die Befugnisnorm des § 2 BNDG, die nähere Vorgaben umschreibt. Diese werden gegenständlich auf Daten begrenzt, die „im Geltungsbereich dieses Gesetzes erhoben“ werden.[16] § 1 Abs. 2 S. 1 BNDG erlaubt nicht den Schluss, dass eine Erhebung oder Auswertung durch den BND mit Hilfe von Einrichtungen, die nicht im deutschen Hoheitsgebiet gelegen sind, keinen rechtlichen Restriktionen nach deutschem Recht unterliegen. Dies wäre mit Art. 10 GG nicht vereinbar[17]. Der hier maßgebende Schutz vor staatlichen Eingriffen gilt dem Kommunikationsinhalt und den Begleitumständen der Kommunikation. Würde der BND

[15] Zu den Rechtsfragen der Datengenerierung durch den BND siehe *Kment*, Grenzüberschreitendes Verwaltungshandeln (2010), S. 718 ff.

[16] Möglicherweise entspricht es internationaler Übung, dass nationale Staatsorgane sich beim Handeln im Ausland nicht durch die für sie maßgebenden nationalen Gesetze gebunden fühlen. Eine solche Sicht muss allerdings für das Handeln deutscher Staatsorgane ausscheiden, da das Grundgesetz keine entsprechende Öffnung vorsieht.

[17] S. dazu *Hermes*, in: Dreier, Grundgesetz, Bd. 1 (2013) Rn. 43 zu Art 10; *Baldus*, in: Epping/Hillgruber, Beck'scher Online-Kommentar GG, Rn. 21 zu Art. 10; *Huber*, Die strategische Rasterfahndung des Bundesnachrichtendienste - Eingriffsbefugnisse und Regelungsdefizite, NJW 2013, S. 2572, 2575; *Caspar*, Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats? In: PinG 01.14, S. 1, 13 f. m.w. Hinw.

als deutscher Hoheitsträger durch Anzapfen eines im extraterritorialen Gebiet verlegten Glasfaserkabels, eines dort stationierten Servers oder unter Inanspruchnahme eines dort tätigen Providers abhören, wäre dies nicht nur dann ein Eingriff in Art. 10 GG, wenn er sich auf einen in Deutschland oder von oder nach Deutschland erfolgenden Kommunikationsverkehr bezöge, sondern auch, wenn die Spähaktionen im Ausland erfolgen.

Eine solche Maßnahme wäre nach dem BNDG insoweit rechtswidrig, als sie nicht zur Erfüllung der gesetzlichen Zwecke erfolgte, insbesondere nicht der „Gewinnung von Erkenntnissen über das Ausland" diente (Art. 1 Abs. 2 S. 1 BNDG), oder wenn sie nicht den Anforderungen der in Art. 1 Abs. 2 S. 2 BNDG in Bezug genommenen Normen entspräche.

II. Insbesondere: Grenzen der Weitergabe von Daten aus Spähaktionen[18]

Derartige Daten dürften in der Folge auch nicht an andere Stellen weitergegeben werden. Ohnehin unterliegt die Weitergabe von Daten durch den BND strengen Anforderungen. Ihm ist es - und dann auch nur mit Zustimmung des Bundeskanzleramtes unter engen Voraussetzungen - erlaubt, die von ihm zulässigerweise erhobenen Daten an ausländische Stellen zu übermitteln. Vorausgesetzt ist, dass dies zur Wahrung außen- oder sicherheitspolitischer Belange der Bundesrepublik Deutschland erforderlich ist (§ 9 Abs. 2 Satz 1 BNDG).

Es gibt noch weitere Normen über die Weitergabe von Daten. So erlaubt Art. 3 des Zusatzabkommens zum NATO-Vertrag die Weitergabe, soweit die Sicherheit von NATO-Truppen in Deutschland betroffen ist. Ferner dürfen bei gemeinsamen Truppeneinsätzen - wie sie etwa in Afghanistan erfolgt sind - Daten übermittelt und es dürfen Daten, die von verschiedenen Diensten erhoben wurden, unter bestimmten Voraussetzungen verbunden werden, so etwa mit dem Ziel, ein Bild über die Lage in bestimmten Gegenden der militärischen Einsatzgebiete zu erstellen. Solche Ermächtigungen aber sind begrenzt. So erlauben sie nicht die pauschale Übermittlung von (Roh-)Daten, auch nicht von Daten, bei denen der Bezug auf die tatbestandlichen Voraussetzungen der Datenübermittlung noch gar nicht festgestellt worden ist oder bei denen der Zweck ihrer Auswertung die Weitergabe nicht rechtfertigt. Die Rechtsbindungen der Weitergabe entfallen für den BND, der ohnehin nur Auslandsaufklärung betreiben darf, auch nicht etwa dann, wenn keine Daten deutscher Staatsbürger betroffen sind.

[18] Zur Datenübermittlung ins Ausland allgemein siehe *Kment* (Fn. 14), S. 686 ff.

Auf die Staatsangehörigkeit kommt es für die Beurteilung der Datenerhebung durch den BND nicht an.

E. Mittelbarer Grundrechtschutz gegenüber dem Handeln Dritter einschließlich auswärtiger Staatsorgane

Eine andere Frage ist, wieweit private Dritte oder Vertreter auswärtiger staatlicher Stellen[19] an Grundrechte gebunden sind[20]. Eine Direktwirkung der Grundrechte ihnen gegenüber scheidet aus. Mittelbar aber wirken sich die Grundrechte aus, soweit ihr Schutzgehalt durch die Normen der allgemeinen Rechtsordnung - wie denen des Datenschutzrechts oder allgemeinen Zivil- oder Strafrechts - so konkretisiert worden ist, dass er gegen Dritte wirkt.

Ausländische Hoheitsträger oder Privatpersonen sind beim Handeln im Anwendungsbereich deutschen Rechts an die deutschen Rechtsnormen gebunden. Das Handeln von Trägern ausländischer Hoheitsgewalt in Deutschland kann darüber hinaus eine Souveränitätsverletzung nach völkerrechtlichen Maßstäben darstellen.[21] Soweit solche Träger nicht durch Abkommen - etwa durch das NATO-Truppenstatut - von der Anwendung deutschen Rechts freigestellt sind, müssen sie vor dem Hintergrund deutscher Jurisdiktionshoheit deutsche Gesetze (also etwa das Telekommunikationsgesetz, die Datenschutzgesetze und das Strafgesetzbuch) und damit auch die in ihnen konkretisierten grundrechtsorientierten Vorgaben befolgen.[22]

Spionagetätigkeit als solche ist zwar völkerrechtlich nicht verboten. Spionagetätigkeit ist aber nach Maßgabe nationaler Gesetze verboten[23] und weitgehend unter Strafe gestellt. Bei Eingriffen in die Privatsphäre sind insbes. §§ 203 sowie 202 a – c StGB einschlägig. Hinzu treten Sanktionsnormen aus dem Datenschutzrecht (§§ 43 Abs. 2, 44 Abs. 1 BDSG) und aus dem Recht der Wirtschaftsspionage (§17 UWG). Anwendbar können ferner die Staatsschutzdelikte (§§ 92 ff. StGB) sein, insbes. §§ 99, 96 Abs. 1, 98, aber auch § 109 StGB.

---

[19] Erfolgt das Handeln aber mit Billigung oder unter Duldung deutscher Staatsorgane, sind die Maßnahmen (auch9 der deutschen Staatsgewalt zuzurechnen, s. dazu etwa BVerfGE 66, 39,62

[20] Überblick über die räumlichen Geltungsbereiche der Grundrechte bei *Badura*, Der räumliche Geltungsbereich der Grundrechte, in: Merten/Papier (Hrsg.), Handbuch der Grundrechte, Bd. II/1 2006, § 47, Rn. 9. sowie *ders.* Bonner Kommentar, Grundgesetz, Kommentierung zu Art. 10, Rn. 86 m. w. Hinw. n Fn. 223; Zur Bindung fremder Hoheitsgewalt an deutsche Grundrechte s. auch *Menzel*, Internationales Öffentliches Recht, 2001, S. 609 f.; *Walter*, Grundrechtsschutz gegen Hoheitsakte internationaler Organisationen, 129 AöR (2004), S. 39 ff.

[21] Hierzu jüngst *Ewer/Thienel*, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, NJW 2014, 30 (31).

[22] So konstatierte das BVerfG im Maastricht-Urteil z. B., es gewährleiste Grundrechtsschutz „in Deutschland und insoweit nicht nur gegenüber deutschen Staatsorganen", BVerfG 89, 155 (174 f.). Vgl. auch OLG Karlsruhe NJW 1992, 642 (643) - im Hinblick auf behauptete Ermittlungsmaßnahmen seitens US-amerikanischer Beamter.

[23] Vgl. auch BVerfGE 92, S. 227, 328 ff.

Wieweit die tatbestandlichen Voraussetzungen durch die Aktionen konkret erfüllt sind, entzieht sich allerdings meiner Kenntnis.

Festzuhalten ist, dass Spionagetätigkeiten nicht dem Schutz der völkerrechtlichen Staatenimmunität im Sinne der allgemeinen Funktionsträgerimmunität unterfallen[24]. Gegenteiliges ist auch nicht dem Urteil des IGH vom 03.02.2012 zu entnehmen[25]. Es betrifft Fragen der zivilrechtlichen Einstandspflicht eines Staates (hier Deutschland) betreffend Entschädigungen im Hinblick auf völkerrechtliche Verbrechen und schwere Menschenrechtsverletzungen. Die Urteilsgründe verdeutlichen, dass der IGH zwischen der Invokation von Staatenimmunität in zivilrechtlichen Verfahren einerseits und Strafverfahren gegen einzelne Amtsträger andererseits differenziert und sich einer Aussage zu letzteren enthält[26]. Der IGH adressiert daher auch nicht die Frage der Strafrechtsimmunität bei Spionage.

Soweit die deutschen Gesetze Eingriffsverbote für Dritte vorsehen oder Eingriffe strafrechtlich sanktionieren, sind diese auch auf Träger auswärtiger Hoheitsgewalt anwendbar. Bei einem Handeln in Deutschland können diese sich ihrerseits nicht auf Hoheitsrechte ihres Landes berufen, zum Teil nicht einmal auf deutsche Grundrechte als Schutzrechte (vgl. Art. 19 Abs. 3 GG).

Die in Deutschland handelnden Ausländer sind auch der deutschen Gerichtsbarkeit unterworfen, auch der Strafgerichtsbarkeit. Selbst bei einem Handeln im Ausland ist deutsches Strafrecht anwendbar, wenn einer der in §§ 5 – 7 StGB Tatbestände erfüllt wird.[27].

Die allgemeinen Schädigungs- bzw. Eingriffsverbote[28], gelten nur insoweit nicht, als eine ausnahmsweise Ermächtigung für Eingriffe besteht. Die für Überwachungsmaßnahmen

[24] Dazu ausführlich *Frowein*, Völkerrechtliche Fragen der Strafbarkeit von Spionen aus der ehemaligen DDR: Gutachten erstattet im Auftrag des Bundesverfassungsgerichts, 1995, S. 18 ff; siehe auch *Verdross/Simma*, Universelles Völkerrecht 3. Auflage 1984 (Neudruck 2010), § 1177; eine - sachlich weitergehende - diplomatische Immunität der handelnden Personen käme nur in Betracht, wenn sie Inhaber diplomatischer Vorrechte wären; auch dann müssten sich die Handelnden aber nach Art. 41 Abs. 1 des Wiener Übereinkommens über diplomatische Beziehungen an das in Deutschland geltende Recht halten. Dass Spionagetätigkeit nicht von dem Grundsatz der Staatenimmunität erfasst wird, bejahen auch *Bothe*, Die strafrechtliche Immunität fremder Staatsorgane 31 ZaöRV (1971), 246 (257); *Herdegen*, Die Achtung fremder Hoheitsrechte als Schranke nationaler Strafgewalt 47 ZaöRV (1987), 221 (224).

[25] IGH, Jurisdictional Immunities of the State (Germany v. Italy), Urteil v. 03.02.2012

[26] So stellt er fest: „… the Court must emphasize that it is addressing only the immunity of the State itself from the jurisdiction of the courts of other States; the question of whether, and if so to what extent, immunity might apply in criminal proceedings against an official of the State is not an issue in the present case." (Rn. 91).

[27] S. dazu etwa *Deiseroth*, Staatliche Internet-Kriminalität im gemeinsamen Europa, Betrifft JUSTIZ 2007, S. 115, 116

[28] Zu diesem Achtungsanspruch siehe *Chesterman*, in Wolfrum (ed.), Max Planck Encyclopedia of International Law, Secret Intelligence, Januar 2009, Abs. 14; *Verdross/Simma*, (Fn.), 24 § 456.

deutscher Behörden geschaffenen Ermächtigungen - etwa im BND-Gesetz, BKA-Gesetz oder G-10G u. a. - räumen Trägern auswärtiger Hoheitsgewalt keine Eingriffsbefugnisse ein.

F. Schutzaufträge und Schutzpflichten deutscher Staatsorgane zur Grundrechtsgewährleistung auch gegenüber dem Handeln auswärtiger Staatsorgane

Aus den Grundrechtsnormen können Schutzpflichten abgeleitet werden, die auf den Erlass von Schutznormen oder anderer geeigneter Schutzvorkehrungen zur Gewährleistung des Freiheitsschutzes der Bürger gegen Eingriffe privater Dritter oder Träger auswärtiger Staatsgewalt gerichtet sind. Schutzpflichten folgen nicht notwendig nur aus Grundrechtsnormen, sondern können auch aus anderen Normen abgeleitet werden.

Solche Schutzaufträge und -pflichten sind im vorliegenden Zusammenhang besonders wichtig, um die Defizite des Freiheitsschutzes auszugleichen, die angesichts globaler Kommunikationsinfrastrukturen und der Möglichkeiten extraterritorial erfolgender Eingriffe in Kommunikation bestehen.

I. Objektiv-rechtliche Gehalte der einschlägigen Grundrechtsnormen

Die für den Schutz der Kommunikationsfreiheiten maßgebenden Grundrechtsnormen haben durchgängig neben ihrer Verbürgung als subjektives Recht den Charakter objektiv-rechtlicher Schutzaufträge[29]. Dies gilt für das Telekommunikationsgrundrecht (Art. 10 GG)[30], das Wohnungsgrundrecht (Art. 13 GG)[31], das Grundrecht auf informationelle Selbstbestimmung[32], die Kommunikationsfreiheit (Art. 5 GG)[33], aber auch weitere eventuell betroffene Grundrechte wie Art. 12 und 14 GG.[34]

II. Insbesondere: Objektiv-rechtlicher Schutz durch das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit der eigenen informationstechnischen Systeme

[29] S. statt vieler BVerfGE 125, 39, 78 m.w.Hnw.
[30] Siehe *Hermes* in: Dreier, Grundgesetz (2013), Art. 10 Rn. 92 m. w. Hinw. in Fn. 402.
[31] Siehe *Hermes* in: Dreier, Grundgesetz (2013), Art. 13 Rn. 120 ff.; siehe auch BVerfGE 89, 1, 11.
[32] Siehe *Dreier*, in: Dreier, Grundgesetz (2013), Art. 2 I, Rn. 94 ff.
[33] Siehe BVerfGE 57, 295, 319; 107, 275, 280 f.
[34] Dazu siehe *Wieland*, in Dreier, Grundgesetz (2013), Art. 12 Rn. 142 ff.; Art. 14 Rn. 195 ff.

Besondere Bedeutung gewinnt das schon erwähnte Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit der eigenen informationstechnischen Systeme.[35] Der bisher über das Grundrecht auf informationelle Selbstbestimmung erreichbare Schutz konkreter Kommunikationsvorgänge ist angesichts der bekannten Gefährdungslagen häufig praktisch nicht realisierbar und greift letztlich nur punktuell[36]. Wirksamer Schutz ist praktisch auf Systemschutz angewiesen.

Es muss daher auf eine Ausgestaltung der informationstechnischen Systeme derart hingewirkt werden, dass sie Sicherheitsanforderungen genügen, die einen Schutz personenbezogener Kommunikation losgelöst von der Möglichkeit der Kenntnisnahme von Eingriffen durch den Betroffenen und damit der individuellen Abwehr gewähren. Außerhalb der durch das Persönlichkeitsrecht geschützten Kommunikationsvorgänge - etwa solche rein wirtschaftlicher Art - wird es darum gehen müssen, entsprechende Aufträge zur Sicherung des Systemschutzes aus anderen Verfassungsnormen (etwa auch Art. 12, 14 GG) abzuleiten.

Die detaillierten Schilderungen der Praxis von NSA und anderen Ausspähorganisationen zeigen - etwa die Wiedergabe der Inhalte der Snowden-Unterlagen durch Rosenbach und Stark[37]-, dass die Spähaktionen nicht nur aus dem „Absaugen“ von Daten aus Glasfaserleitungen bestanden. Vielmehr sind erhebliche Eingriffe in die Software, aber auch die Hardware der IuK-Infrastrukturen erfolgt, darunter auch der Einbau von sog. Trojanern und anderes mehr. Die Eingriffe in die informationstechnischen Systeme waren erheblich vielfältiger, nachhaltiger und tiefgreifender als der geplante Einsatz der Trojaner zur Online-Überwachung, die Ausgangspunkt der Entscheidung des BVerfG war. Das Gericht hat die Notwendigkeit von Systemschutz erkannt. Jetzt ist es an der Zeit, Grundlagen für seinen Ausbau zu schaffen, die es ermöglichen, dass auch den neu bekannt gewordenen Gefährdungen begegnet werden kann.

Dabei kann auch an die objektiv-rechtliche Reichweite der vom BVerfG entwickelten Grundrechtskonstruktion angeknüpft werden. Diese ist vom BVerfG zwar nicht ausdrücklich thematisiert worden, da es in der Entscheidung ausschließlich um subjektiv-rechtlichen Grundrechtsschutz ging. Die Möglichkeit einer auch objektiv-rechtlich bedeutsamen Reichweite der neuen Grundrechtskonkretisierung folgt aber schon daraus, dass diese Gewährleistung aus Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG entwickelt worden ist, also Normen mit (auch) objektiv-rechtlichen Gehalten.

[35] BVerfGE 120, 274, 313 ff.
[36] Zu Schutzgrenzen dieses und anderer Grundrechte s. BVerfGE 120, 274, S. 302 ff.
[37] *Rosenbach/Stark*, Der NSA Komplex, 2014

Die Notwendigkeit einer über den subjektiv-rechtlichen Rechtsgüterschutz hinausreichenden Reichweite der Gewährleistung wird durch die gegenständlichen Schutzobjekte belegt, die „informationstechnischen Systeme". Die Unantastbarkeit der Integrität und Vertraulichkeit der eigengenutzten informationstechnischen Systeme ist Voraussetzung effektiven Grundrechtsschutzes der Kommunikation, die mit Hilfe solcher Systeme erfolgt. Gerade weil der Grundrechtsschutz um der Freiheit des individuellen Kommunikationsverhaltens willen gewährleistet wird, ist der Schutz wichtiger infrastruktureller Bedingungen moderner Telekommunikationstechniken als Schutz der realen Verwirklichungsbedingen von Freiheit unabweisbar[38]. Der über das Grundrecht angestrebte Vertraulichkeits- und Integritätsschutz bedarf daher auch positiver Vorkehrungen zu seiner Verankerung im informationstechnischen System selbst, und zwar in einer den aktuell bekannt gewordenen Gefährdungen angemessenen Weise.

III. Gewährleistung der Funktionsfähigkeit der IuK-Infrastrukturen (Art. 87f GG)

Schutzaufgaben sowie Schutzaufträge können sich auch aus anderen Normen ergeben. Speziell auf die Gewährleistung der Funktionsfähigkeit der IuK-Infrastrukturen - und damit auf Systemschutz, nicht speziell auf Persönlichkeitsschutz - ist (wenn auch nur in begrenztem Umfang) Art. 87f GG bezogen (Sicherung angemessener und ausreichender Telekommunikationsdienstleistungen). Die in der Norm benutzten Begriffe verdeutlichen, dass es dem Verfassungsgeber um die Sicherung einer hinreichenden Qualität der Kommunikationsinfrastruktur ging. Allerdings wurde bei der Schaffung der Norm in erster Linie an das Risiko gedacht, die Telekommunikationsunternehmen könnten aus ökonomischen Erwägungen dünn besiedelte, strukturschwache Gebiete nicht zu angemessenen Preisen versorgen wollen. Die zwischenzeitlich veränderten Verhältnisse rücken die Notwendigkeit auch anderer Sicherungen der Qualität der Telekommunikationsleistung in den Blick. Angemessen ist eine Kommunikationsversorgung nur, wenn sie auch Schutz vor Ausspähung, Manipulation und sonstigen Beeinträchtigungen freier Kommunikation gewährt. Der Maßstab der Angemessenheit kann in systematischer Interpretation auch unter Rückgriff auf die Garantien der Kommunikationsgrundrechte (s. o. B)inhaltlich aufgefüllt und gegebenenfalls im Zuge einer Rechtsfortbildung auf neue Lagen erstreckt werden.

[38] *Greve*, Netzinfrastruktur und Kommunikationsfreiheit, K&R 2013, 87, 89 sieht den Schutz elektronisch vernetzter Kommunikation als „Grundrechtsvoraussetzung" an.

Soweit die von Art. 87f GG erfassten Anbieter zur Erbringung der Telekommunikationsdienstleistungen Infrastrukturen betreiben, muss der Bund im Rahmen seiner Möglichkeiten die Angemessenheit der Kommunikationsversorgung gewährleisten. Wenn Schutz vor Ausspähung oder Manipulation etwa durch auswärtige Staaten anderweitig nicht erreicht werden kann, kommen dafür auch z. B. Vorgaben für ein europainternes Routing oder andere Arten der Dezentralisierung oder sonstiger Möglichkeiten zur Nutzung von sicheren Netzen in Betracht, die von globalen Infrastrukturen, soweit diese keine sichere Kommunikation ermöglichen, getrennt sind. Der Aufbau der globalen und hoch vernetzten Kommunikationsinfrastruktur des Internet war und ist eine großartige technologische und soziale Innovation. Dies anzuerkennen, schließt aber nicht das Nachdenken darüber aus, ob und wie die durch neue technologische Entwicklungen sowie neue Geschäftsmodelle bedingten neuen Gefährdungspotentiale auch durch Änderungen der „Netzphilosophie“[39] reduziert werden und durch teilweisen Um-/Neubau der Netze die vielen Chancen der Informationsgesellschaft besser genutzt werden können.

IV. Sicherheitsanforderungen an informationstechnische System (Art. 91c GG)

Eine weitere einschlägige Norm außerhalb des Grundrechtskatalogs ist Art. 91c GG. Sie regelt die Zusammenarbeit von Bund und Ländern bei der Planung, Errichtung und bei dem Betrieb informationstechnischer Systeme, die für deren Aufgabenerfüllung benötigt werden.[40] Diese Norm steht im Zusammenhang der Verwaltungskooperation auch mit der EU, dem Grundrecht auf eine gute Verwaltung (Art. 41 Grundrechtecharta) sowie den Anforderungen der europäischen Dienstleistungsrichtlinie.[41]

Gesichert werden sollen insbesondere die Interoperabilität und Sicherheit dieser Infrastrukturen. Soweit Bund und Länder keine physisch von den allgemeinen Infrastrukturen getrennten Teilnetze betreiben und nutzen, erstreckt die Aufgabe sich auf die Nutzung der allgemein nutzbaren Netze. Dies betrifft auch die Kommunikation mit den Bürgern, etwa im Rahmen des E-Government. Insofern müssen sich Sicherheitsanforderungen auch auf Kommunikation außerhalb des internen Behördenbetriebs beziehen. Es besteht kein

[39] Aus den vielen insoweit diskutierten Neukonzeptionen sei nur eine benannt: *Lanier,* Wem gehört die Zukunft? 2014 – ohne dass dies eine Stellungnahme zu seinen konkreten Ideen sein soll.
[40] Siehe zu Art. 91c GG allgemein auch *Schliesky*, Art. 91c GG als archimedischer Punkt staatlicher Informationsverarbeitung und Wissensgenerierung im Bundesstaat, in: Zeitschrift für Staats- und Europawissenschaften 2013, S. 281 ff.
[41] So *Mager*, in v. Münch/Kunig, Grundgesetzkommentar (2012), Rn. 4 zu Art. 91c GG.

nachvollziehbarer Grund, die Anforderungen an die „Sicherheit“ nicht auch auf die Integrität und damit den Schutz vor Eingriffen in konkrete Kommunikationsvorgänge, aber auch die Integrität der Netze als solche zu beziehen.

V. Übergreifende Gewährleistungsaufgabe als Folge systematischer Interpretation der Verfassungsnormen

Angesichts der vielen Facetten der Bedeutung der IuK-Infrastrukturen für Staat und Gesellschaft und die individuellen Bürger und angesichts unterschiedlicher Gefährdungslagen liegt es nahe, die verschiedenen Normen ungeachtet ihrer verbleibenden Besonderheiten auch in ihrem Zusammenspiel und damit als Gesamtkomplex zu sehen. Individualrechtsschutz und Systemschutz gehören zusammen. Soll das bisherige Schutzniveau gewährleistet oder muss es erhöht werden, ist es unabdingbar, dass die verschiedenen Verfassungsnormen (Art. 2 Abs. 1, 1 Abs. 1, 10, 87f, 91c GG) - unter ergänzendem Rückgriff auf die allgemeinen Staatszielbestimmungen (Art. 20 GG), insbesondere die der Demokratie - im Zuge systematischer Interpretation als Grundlage für eine übergreifende Gewährleistungsaufgabe des Staates im Hinblick auf den Schutz der Funktionsfähigkeit einschließlich der Sicherheit informationstechnischer Systeme verstanden werden.

Verschiedene normative Bausteine ergänzen sich in dem Gewährleistungsauftrag. Es mag zwar für einzelne Rechtsfolgen, nicht aber für die Aufgabe selbst, von Bedeutung sein, in welchen rechtlichen Kontext die einzelnen Bausteine je für sich geordnet sind. Für das Bestehen der Aufgabe ist es insbesondere nicht entscheidend, wieweit ein Bürger aufgrund eines Grundrechts gegebenenfalls Individualrechtsschutz in Anspruch nehmen kann. Auch ist die Maßgeblichkeit normativer Aufgaben nicht zwingend an eine rechtliche Sanktionierbarkeit von Fehlverhalten gekoppelt. Entscheidend ist die Rechtspflicht der zuständigen Staatsorgane, sich der Aufgabe anzunehmen. Auf welchem Wege - ob mit Hilfe der Gerichte oder nur mit Hilfe politischer Sanktionen - Staatsorgane gegebenenfalls zur Erfüllung der Pflichten angehalten werden können, ist zwar praktisch nicht unwichtig, aber für die normative Maßgeblichkeit der Aufgabe nicht entscheidend. Allerdings kann die Verletzung der Schutzaufgaben Sanktionen nach sich ziehen, so durch das Parlament, gegebenenfalls auch unter Nutzung einer Organklage beim Bundesverfassungsgericht (Art. 93 Nr. 1 GG), einer abstrakten Normenkontrolle (Art. 93 Nr. 2 GG) oder in Form von Entschließungen oder politischen Sanktionen durch die Parlamente.

G. Einwirken der Schutzaufgabe auch auf Handeln im internationalen Kontext

Schutzaufträge und -pflichten deutscher Staatsorgane wirken auch - soweit zur Gewährleistung effektiven Schutzes erforderlich - in den internationalen/globalen Raum hinein und umfassen beispielsweise nachhaltige Bemühungen um Vorkehrungen zum Grundrechtsschutz auch gegenüber dem Handeln von Trägern anderer Staatsgewalten. In Rechtsprechung und Literatur[42] herrscht jedenfalls die Auffassung vor, dass die Bundesrepublik Deutschland aufgrund der objektiv-rechtlichen Schutzfunktion von Grundrechten verpflichtet sein kann, „sich fordernd und schützend auch außerhalb des deutschen Hoheitsgebiets für seine Staatsangehörigen einzusetzen und ausländischen Gefahrenquellen entgegenzuwirken".[43] Schutzpflichten bestehen jedenfalls im Hinblick auf Gefährdungen von Grundrechten, die von fremden Staaten oder internationalen Organisationen ausgehen.

Allerdings erfassen die aus deutschem Recht abgeleiteten Schutzaufträge/-pflichten nicht alle weltweiten Kommunikationsvorgänge. Die Art und Weise des abwehrrechtlichen Grundrechtsschutzes einerseits und die inhaltliche Reichweite von Schutzpflichten andererseits müssen nicht deckungsgleich sein. Auch wenn die Erstreckung des Abwehrrechts gegenüber Eingriffen deutscher Staatsorgane auch auf reine Auslandskommunikation mit vollem Schutzniveau anzuerkennen ist[44], impliziert dies nicht notwendig eine entsprechende Erstreckung der Schutzpflicht. So hat das BVerfG[45] formuliert, dass der Grundrechtsschutz bei transnationalem bzw. extraterritorialem Handeln staatlicher Stellen auch vom „Umfang der Verantwortlichkeit und Verantwortung deutscher Staatsorgane" abhänge. Bei der Entfaltung einzelner Gewährleistungsgehalte muss darum jeweils bestimmt werden, welche Folgen solchen Handelns der deutschen Staatsgewalt zurechenbar sind und welche transnationalen Schutzleistungen sie zu erbringen haben und überhaupt erbringen können.

Dementsprechend muss ein Anknüpfungspunkt für die Schutzaufgaben nach deutschem Rechtsgegeben sein (Deutschlandbezug). Wieweit dies der Fall ist, bedarf hier keiner grundsätzlichen Klärung. Ein hinreichender Anknüpfungspunkt ist jedenfalls im Hinblick auf

---

[42] Dazu siehe BVerfGE 77, 170, 214 ff.; 92, 26, 47. Siehe ferner die Nachweise bei *Giegerich*, Verfassungsgerichtliche Kontrolle der auswärtigen Gewalt im europäisch-transatlantischen Verfassungsstaat, in: Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, 1997, S. 409, 550 f. sowie bei *Kment* (Fn. 14), S. 177 f.

[43] So *Ress*, Der internationale diplomatische Schutz und die Grund- und Menschenrechte, in: Merten/Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Bd. VI/2, 2009, Rn. 92.

[44] S. dazu – bezogen auf Art. 10 GG – die Hinweise in Fn. 17. Entsprechendes gilt für andere Grundrechtsnormen des Kommunikations- und Persönlichkeitsschutzes, deren Schutzbereich nicht auf Deutsche begrenzt ist

[45] BVerfGE 100, 313, 362 f

Kommunikationsvorgänge gegeben, bei denen die an ihnen Beteiligten (Kommunikatoren und/oder Rezipienten) im deutschen Rechtsraum handeln und schon deshalb auf den Schutz vor Eingriffen rechnen dürfen. Das ist der Fall, wenn sie mit Rezipienten in Deutschland oder im Ausland kommunizieren oder wenn ein Kommunikationsinhalt, der aus dem Ausland stammt, in Deutschland empfangen werden soll. Der Ort des Eingriffs ist für die Bestimmung von Schutzpflichten als solchen nicht maßgeblich, soweit ein hinreichender Deutschlandbezug des grundrechtlich geschützten Verhaltens gegeben ist. Der Ort kann aber Bedeutung für die konkrete Art der Umsetzung der Schutzplichten haben.

Die Nichtwahrnehmung von staatlichen Schutzaufgaben (also ein staatliches Unterlassen) kann zwar nur unter besonders engen Voraussetzungen[46] unter Nutzung subjektiver Rechte der Bürger gerichtlich geahndet werden[47]. Eine Rechtsverletzung durch Unterlassen von Schutzvorkehrungen ist inhaltlich aber nicht von der Sanktionierbarkeit durch subjektiven Rechtsschutz abhängig.

H. Europarechtliche Anknüpfungspunkte für Schutzvorkehrungen

„Andockstellen“ für einen Ausbau der Schutzvorkehrungen bestehen nicht nur national, sondern auch im europarechtlichen sowie im völkerrechtlichen Bereich.

Im EU-Bereich ist neben den europäischen Verträgen auch die Grundrechtecharta heranzuziehen. Im Unionsrecht sind insbesondere Art. 16 Abs. 1 und Art. 18 Abs. 1 AEUV sowie Art. 1, 6, 7, 8 und 11 der EU-Grundrechtecharta, der nunmehr der Rang Primärrechts zukommt,[48] maßgebend, aber auch die unionsrechtlichen Grundfreiheiten (insbesondere Art. 26 bis 66 AEUV) sowie die Spezialregelungen über den Raum der Freiheit, der Sicherheit und des Rechts (Art. 67 bis 89 AEUV). Auch die Grundrechte der EMRK sind gemäß Art. 6 Abs. III EUV als allgemeine Grundsätze als Teil des Unionsrechts zu behandeln.

Die hohe Bedeutung effektiven Persönlichkeitsschutzes hat der EuGH jüngst in seinen Entscheidungen zur Vorratsdatenspeicherung[49] sowie zu Pflichten von Google im Hinblick auf den Umgang mit personenbezogenen Daten (dort insbesondere auf das „Recht auf Vergessenwerden“)[50] betont. Diese Entscheidungen betreffen zwar nicht direkt die hier zu

[46] Vgl. etwa BVerfGE 79, 174, 202; 92, 26, 46
[47] Vgl. etwa BVerfGE 77, 170, 214; 92, 26, 46; 125, 39, 78.
[48] Vgl. Art. 6 Abs. 1 EUV.
[49] EuGH , Urteil v. 8. April 2014, C-293/12 (Digital Rights Ireland)
[50] EuGH, Urteil v. 13.Mai 2014, C-131/12 (Google Spain)

untersuchende Problematik. Sie werden aber auf Grundsätze gestützt, die in vielerlei Hinsicht Orientierung auch für die rechtliche Beurteilung von sonstigen Beeinträchtigungen des Persönlichkeitsschutzes und der digitalen Kommunikation bei transnationalen Vorgängen der Kommunikation geben.

Von Bedeutung sind auch die Ausführungen der Google-Entscheidung über die Anwendbarkeit des europäischen Rechts in Anknüpfung an den Sitz einer Zweigniederlassung in einem Mitgliedstaat (also nicht an den Hauptsitz des Unternehmens einer Suchmaschine) und an eine in dem betreffenden Mitgliedstaat erfolgende Betätigung (dort konkret etwa der Verkauf von Werbeflächen)[51], mit Folgen für die Maßgeblichkeit europäischen Rechts und für den Gerichtsstand. Die Ausführungen zum Schutz durch Europarecht bei Kommunikationsvorgängen mit Europabezug haben mittelbar auch Bedeutung für die Beurteilung, wann ein außerhalb des europäischen Raumes durchgeführter Eingriff in Kommunikationsvorgänge nach europäischem Recht unter Einschluss der Grundrechte zu beurteilen ist, sofern Kommunikation mit Europabezug betroffen ist, also insbesondere solche, die zwischen Bürgern der Mitgliedstaaten erfolgt oder bei der diese mit Bürgern außerhalb des EU-Bereichs kommunizieren. Die vom EuGH geforderte Sicherstellung eines hohen Schutzniveaus[52] muss auch bei der Klärung berücksichtigt werden, ob und mit welchen Folgen ein Eingriff in Kommunikationsvorgänge (auch) nach europäischem Recht zu beurteilen ist.

Die Überlegungen des EuGH sind für die rechtliche Beurteilung, nämlich die Anwendung unionalen Rechts und mittelbar des nationalen Rechts, insbesondere bedeutsam, wenn solche Unternehmen wie Google mit Behörden auswärtiger Staaten – wie es offenbar in der Vergangenheit geschehen ist – bei der Erfassung und Weitergabe von Daten oder gar der Einrichtung/Manipulation der software oder hardware informationstechnischer System (freiwillig oder erzwungen) so kooperieren, dass Zugang zu oder gar direkter Zugriff auf Meta- oder Inhaltsdaten von Kommunikation gewährt oder ermöglicht wird, die dem europäischen Grundrechtsschutz unterliegt (Europabezug). Diese Aussage betrifft nicht die Zugänglichkeit der öffentlich über Suchmaschinen auffindbaren Informationen. Sie gilt dem Zugriff auf nicht öffentlich zugängliche Daten, die beispielsweise bei der Nutzung von Suchmaschinen durch die Nutzer anfallen, aber auch beim Zugriff auf die ggf. vom Suchmaschinenbetreiber erfolgten weiteren Auswertungen, etwa durch Erstellung von Persönlichkeitsprofilen[53], die von diesem

[51] AaO, Rn 48, 55 – 57.
[52] AaO, Rn 10,66)
[53] Dazu vgl. auch EuGH, aaO, Rn 80.

für eigene Zwecke oder zum „Verkauf“ an Dritte erstellt werden. Bei solchen Kooperationsakten im Geltungsbereich des europäischen Rechts sind auch auswärtige Unternehmen, die eine Niederlassung in der EU haben und hier ihr Geschäftsmodell verwirklichen, an die hier geltenden Bestimmungen, so des Datenschutzrechts, gebunden.

Ob und wieweit die Normen des nationalen und des EU-Rechts Schutz- und Gewährleistungspflichten enthalten, ist jeweils durch Einzelanalyse zu erfassen.[54] Angesichts der Bedeutung von Schutz- und Gewährleistungsaufträgen für die Verwirklichung der Grundrechte und -freiheiten in der EU sowie der Aufgabe der Förderung der Europäischen Integration ist bei der Bestimmung der rechtlichen Maßstäbe auch die Frage der Verwirklichung der allgemeinen Rechtsgrundsätze des EU-Rechts einzubeziehen. Schließlich beeinflussen Schutzpflichten auch die Erfüllung des Auftrags zum Auf- und Ausbau transeuropäischer Netze der Telekommunikation (Art. 170 ff. AEUV).

In all diesen Bereichen besteht Potential zur Reaktion auf die hier behandelten Gefährdungspotentiale, die ohne rechtliche Antworten zu dem Risiko führen, dass das grundrechtliche Schutzniveau als praktische Folge neuer technologischer Entwicklungen im europäischen Bereich praktisch abgesenkt wird.

Wirksamer Schutz ist zum Teil auf der Ebene des EU-Rechts ist – auch durch Schaffung neuer Normen unter Einschluss von Strafrechtsnormen - möglich, in Vielem aber angesichts der Globalität der Gefährdungssituation nur durch gemeinsames Handeln der Mitgliedsstaaten und, soweit andere Staaten einbezogen werden müssen, durch internationale Abkommen. Die nationalen und europarechtlichen Schutzaufträge sind auch dahingehend auszulegen, dass die Organe und Institutionen der EU, aber ebenfalls die der Mitgliedsstaaten sich der Aufgabe stellen müssen, die Schutzaufträge auch in dem internationalen Bereich umzusetzen. Aus ihnen folgen Handlungsaufträge zur Schaffung geeigneter Vorkehrungen, insbesondere internationaler Vereinbarungen.

I. Völkerrechtliche Anknüpfungspunkte für Schutzvorkehrungen

[54] Siehe etwa für den Bereich der europäischen Menschenrechtskonvention *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention (2012), S. 138 ff., Zu den EU-Grundfreiheiten siehe etwa *Papier*, Drittwirkung der rundrechte, in Merten/Papier (Hrsg.) Bd. II 2006, § 55 Rn. 49 ff.; *Calliess*, Schutzpflichten, in Merten/Papier (Hrsg.), Handbuch der Grundrechte, Bd. II 2006, § 44, Rn. 17. Zu grundsätzlichen Fragestellungen insbesondere zur Grundrechtecharta siehe auch *Seifert*, Horizontale Wirkung von Grundrechten, in. Europäische Zeitschrift für Wirtschaftsrecht 2011, S. 698 ff.; *Klatt*,Positive Obligations under the European convention on Human Rights, in: ZaöRV 2011, p. 691 et eeq.

Vor Spähaktionen seitens auswärtiger Gewalt auf deutschem Boden schützt das Völkerrecht das Individuum zunächst reflexartig über den Grundsatz staatlicher Souveränität und somit territorialer Integrität, der einem Staat jedwede Aktivitäten auf dem Territorium eines anderen Staates untersagt, sofern es an einer Erlaubnisnorm hierfür fehlt.[55] Über diesen bloßen Reflex hinaus sind auf völkerrechtlicher Ebene jedoch auch (jedenfalls grundsätzlich) Schutzplichten anerkannt.[56] Ausgeprägt ist insbesondere der sogenannte diplomatische (vor allem konsularische) Schutz, etwa bei Strafverfolgung oder der Beschlagnahme privaten Eigentums.[57] Der diplomatische Schutz hat eine lange Tradition und wird u. a. auch grundrechtlich begründet.[58]

Der diplomatische Schutz ist völkerrechtlich betrachtet zunächst ein Recht zwischen Staaten. Ein Anspruch des Individuums gegenüber seinem Heimatstaat auf Ausübung diplomatischen Schutzes wird traditionellerweise als eine Frage innerstaatlichen Rechts, primär des Verfassungsrechts,[59] nicht so sehr des Völkerrechts, eingeordnet.[60] Ansätze in Richtung einer stärkeren völkerrechtlichen Individualisierung dieses Rechts sind jedoch feststellbar: So sprach der IGH[61] dem konsularischen Schutz in der *LaGrand*-Entscheidung insoweit eine subjektivrechtliche Komponente zu, als er dem Individuum einen Anspruch auf effektive Wahrnehmung dieses Schutzes durch seinen Heimatstaat gegenüber einer fremden Hoheitsgewalt zugestand. In diesem Sinne befördert Völkerrecht jedenfalls innerstaatlich begründete Schutzpflichten und effektiviert deren grenzüberschreitende Verwirklichung. Die normativen Prämissen dieses Schutzes können im Zuge der Rechtsfortbildung auch auf die hier behandelte Gefährdungslage erstreckt werden. Ziel (innovativen) Bemühens wäre es, dieses anerkannte Rechtsinstitut so weit zu entwickeln, dass Schutz über die bisher erfassten Anwendungsfälle hinaus sich auch gegen solche Eingriffe in Kommunikationsvorgänge realisieren lässt, die auf fremden oder exterritorialem Gebiet gegen die eigenen Bürger erfolgen.

---

[55] PCIJ, Case of the S. S. Lotus (Frankreich/Türkei), PCIJ Series A No. 10, S. 18.
[56] Vgl. *Seibert-Fohr*, Die völkerrechtlicher Verantwortung des Staates für Handeln von Privaten, in: Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, 2013, S. 43 ff., 49 ff., 55 ff.; *Koenen*, Staatliche Schutzpflichten (2012) S. 201 ff. und passim; *Badura*, Räumlicher Geltungsbereich (s.o. Fn. 20), Rn. 7.
[57] Dazu siehe etwa *Kment*, (s.o. Fn 14), S. 177 m. Nachw. in Fn. 93 f.
[58] Siehe *Kment*, (s.o. Fn 14), S. 177 m. Fn. 94.
[59] Der Schutz erstreckt sich sogar auf Nichtstaatsangehörige, vgl. *Kleinlein/Rabenschlag*, Auslandsschutz und Staatsangehörigkeit, 67 ZaöRV (2007), 1277 (insb. 1301 ff.).
[60] Vgl. *Geck*, Der Anspruch des Staatsbürgers auf Schutz gegenüber dem Ausland nach deutschem Recht, 17 ZaöRV (1957), S. 476 ff.
[61] IGH, LaGrand Case, Judgment of 27 June 2001, Germany v. United States of America, ICJ-Reports 2001, S. 464 ff.

Im Hinblick auf die mit Hilfe der TK-Infrastrukturen verwirklichten Kommunikationsfreiheiten stehen die Kommunikationsinhalte, aber auch die Metadaten, im Zentrum des Schutzbedarfs. Erfolgt ein Eingriff in die durch die hier einschlägigen deutschen Grundrechte geschützte Kommunikation im Ausland, lässt sich die Grundidee des konsularischen Schutzes aktivieren, die darin besteht, die Bürger auch außerhalb des eigenen Landes zu schützen. In der Folge müsste der Staat - jedenfalls qua Verfassungsrechts – sich bemühen, Schutz im Rahmen seiner Möglichkeiten dort zu gewähren, wo der Eingriff gegen einen nach deutschem Recht grundsätzlich geschützten Träger erfolgt. Die eingreifende auswärtige Gewalt müsste die effektive Verwirklichung dieses Schutzes innerhalb ihres Hoheitsbereichs nach der Ratio der *LaGrand*-Entscheidung ermöglichen. Um dies erreichen zu können, muss der traditionelle Schutz der Bürger in fremden Staaten auf die neue Gefährdungslage im Kommunikationsbereich angepasst, das heißt erweitert, werden. Dies bedarf der völkerrechtlichen Fortbildung des Schutzauftrags, möglichst abgesichert auch über völkerrechtliche Verträge.

Der Anpassung an die neu bekannt gewordene Gefährdungslage harren auch traditionelle völkerrechtliche Verbürgungen in den internationalen Menschenrechtspakten. Der internationale Pakt über bürgerliche und politische Rechte, den auch die USA ratifiziert haben, gewährleistet in Art. 17 das Recht auf Privatleben und Freiheit der Korrespondenz[62] sowie in Art. 9 Abs. 1 das Recht auf Meinungs- und Informationsfreiheit. Den Bürgerrechtspakten werden objektiv-rechtliche Dimensionen zugeschrieben.[63] Verschwiegen werden darf allerdings nicht, dass es erhebliche Schwierigkeiten bei der Durchsetzung der Vorgaben der Menschenrechtspakte gibt. Zugleich soll aber auch betont werden, dass Schutzaufträge im Bereich der Bürgerrechtspakte in der Vergangenheit inhaltlich weiterentwickelt wurden, wenn sich neuartige Gefährdungen ergaben. Diese Grundhaltung kann auch zur Aktualisierung für den hier behandelten Bereich der Gefährdungen von Bürgerrechten im Feld von Information und Kommunikation genutzt werden.

Weiterer Quell völkerrechtlicher Schutzpflichten sind - jedenfalls für die Konventionsstaaten - Art. 8 (Recht auf Achtung des Privat- und Familienlebens) und Art. 10 (Schutz der Meinungsfreiheit) der EMRK. Der EGMR erkennt die Schutzdimension der EMRK-

[62] Die Datenerhebung gilt als Eingriff in Art. 17 Abs. 1 IPbpR, vgl. UN-Menschenrechtsausschuss, Allgemeine Anmerkung Nr. 16, U.N. Doc. HRI/GEN/1/Rev.1 (1994), S. 21 (1994), Rn. 8 [abrufbar unter www1.umn.edu/humanrts/gencomm/hrcom16.htm, zuletzt besucht April 2014]; *Nowak*, U. N. Covenant on Civil and Political *Rights*, CCPR Commentary, 2. Aufl. (2005), Art. 17, Rn. 47 f.
[63] Siehe etwa *Nowak*, U. N. Covenant (2005), S. 379 ff., 448 f.

Verbürgungen grundsätzlich - wenn auch mitunter kasuistisch - an.[64] Diese lassen sich dogmatisch im Hinblick auf die rechtliche Bewältigung gegenwärtiger Bedrohungen fruchtbar machen. Die Garantien der EMRK sind – wie erwähnt – über Art 6 Abs. 3 EUV auch im unionalen Recht von Bedeutung, aber auch im deutschen Verfassungsrecht[65]

J. Gestaltungsspielräume für die Umsetzung der Schutzaufgaben

Angesichts der Aufzählung verschiedener Handlungsfelder darf aber nicht übersehen werden, dass die Staaten als Völkerrechtsobjekte, aber auch die EU-Organe bei der Umsetzung von Schutzaufgaben über einen weiten Gestaltungsspielraum verfügen.[66] Die Gestaltungsspielräume werden häufig in Richtung der Gewährung nur von Minimalschutz genutzt. Ein Vorgehen im Interesse effektiven Freiheitsschutzes würde demgegenüber darauf zielen, den Gestaltungsspielraum möglichst weitgehend auszufüllen, soweit relevante Gefahrenlagen abzuwehren sind.

Wegen der großen Bedeutung der Freiheit der Kommunikation mit Hilfe der IuK-Infrastrukturen dürfte kein Anlass bestehen, für die deutschen und europäischen Organe schon grundsätzlich die Frage des „Ob“ von Schutzvorkehrungen zu verneinen. Das „Wie“ allerdings ist aufgrund des weiten Gestaltungsspielraums grundsätzlich ihnen überlassen. Zu beachten sind aber die normativen Orientierungen, die insbesondere aus nationalem Verfassungsrecht sowie dem primären und sekundären Europarecht folgen, dort auch aus den inhaltlichen Vorgaben, die etwa in Erwägungsgründen der einschlägigen Normen aufgeführt sind.

Orientierungen folgen auch aus der schon erwähnten Google-Entscheidung des EuGH[67] und den dort unter Rückgriff u.a. auf die EU-Grundrechte-Charta und die Richtlinie 95/46 enthaltenen Grundsätze über Persönlichkeitsschutz und die Gewährung hinreichender Rechtsschutzmöglichkeiten.

Der dort im Hinblick auf einen kommerziellen Anbieter von Dienstleistungen und Verwerter von Daten entschiedene Fall unterscheidet sich zwar in der Konstellation von der hier behandelten Problematik hoheitlicher Beeinträchtigung von Freiheitsrechten. Das Urteil konkretisiert aber Gefährdungslagen und Schutzbedarfe aus Anlass von Gefährdungen des

[64] Vgl. *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, 5. Aufl.2012, , § 19 m. w. Hinw.; *Frenz*, Handbuch Europarecht, Band IV, 2009, Rn. 360.
[65] S. BVerfGE 111, 307
[66] Anerkannt auch vom BVerfG, siehe etwa BVerfGE 77, 87, 106; 110, 141, 157 f.; 117, 163, 183; 121, 317, 350;
[67] EuGH, Urteil v. 13.5.2014, C-131/12 (Google Spain)

Persönlichkeitsrechts im Kontext transnationaler/globaler Kommunikation. Gegenüber solchen oder ähnlichen Gefährdungen, die von Trägern auswärtiger Hoheitsgewalt ausgehen, muss es e ebenso effektiven Schutz geben, wie vor Gefährdungen, die vom Verhalten kommerzieller Dienstleister ausgehen.

Hier auf die Schaffung von effektiven Schutzvorkehrungen hinzuwirken, ist eine Aufgabe der EU - etwa im Rahmen der geplanten Novellierung des europäischen Datenschutzrechts sowie der Neuverhandlung (oder Aufkündigung) der Safe-Harbor-Absprache oder eines Swift-Abkommens u.ä. Es ist aber auch eine Aufgabe der deutschen Staatsorgane, sowohl auf die Inhalte der geplanten Datenschutznovellierung und internationaler Vereinbarungen einzuwirken als auch eine Ausgestaltung deutschen Rechts im Sinne der Schutzverstärkung vorzunehmen.

Darüber hinaus gehört es in den Bereich der Wahrnehmung staatlicher Schutzaufgaben, die im nationalen Sicherheits- und Ordungsrecht bestehenden Befugnisse zur Gefahrenabwehr/-vorsorge auch zugunsten der Bürger einzusetzen, die von Spähmaßnahmen betroffen sind oder sein können. Die oben (E) aufgeführten Strafrechtsnormen sind Bestandteil der öffentlichen Sicherheit; sie dienen Schutzgütern, deren Schutz vor Eingriffen den besonderen und den allgemeinen Ordnungs- und Polizeibehörden im Rahmen ihrer Aufträge zum Schutz von Rechten oder allgemein zur Gefahrenabwehr/-vorsorge anvertraut ist. Zu deren Aufgaben gehört das Ergreifen von Maßnahmen zur effektiven Verhinderung von Straftaten der Persönlichkeitsverletzung u.ä.

Davon rechtlich getrennt zu beurteilen sind die Aufgaben der Strafverfolgung. Hier ist das Legalitätsprinzip bei der Strafverfolgung umzusetzen. Die in § 153 c und d StGB enthaltenen Möglichkeiten des Absehens von der Strafverfolgung aus Gründen überwiegender öffentlicher Interessen o.ä. ändern nichts an der soeben erwähnten Aufgabe ordungsbehördlicher Gefahrenabwehr. Die Ermächtigungen zum Absehen von der Strafverfolgung sind lediglich strafprozessualer Art. Auch sie sind unter Beachtung der geschilderten Schutzpflichten auszulegen und deshalb gegebenenfalls nicht zu nutzen, wenn dadurch Schutzaufträge vernachlässigt werden. Ausweislich der bisher bekannt gewordenen – vom NSA-Ausschuss weiter aufzuklärenden – Informationen über Reichweite, Zahl und Tiefe der Spähaktionen und deren intensiv beschränkende Einwirkung auf die Freiheitsrechte der Bürger dürfte der Ermessensspielraum bei gehöriger Berücksichtigung der Schutzaufträge aus den einschlägigen Grundrechtsnormen deutlich eingeengt sein.

Zusammen fassend: Trotz Anerkennung von Gestaltungsspielräumen besteht die Pflicht, für zielführende Maßnahmen zu sorgen, also solche, die Grundrechtschutz real ermöglichen. Dazu gehören Maßnahmen der Schutzgewährung im Einzelfall, aber auch Vorkehrungen mit dem Ziel, die Sicherheit informationstechnischer Systeme als solcher gegenüber Eingriffen zu gewährleisten/erhalten. Insgesamt besteht gegenwärtig ein erheblicher Handlungsbedarf.

K. Schlussbemerkung

Die einzelnen Staaten haben die Aufgabe, ihr nationales Instrumentarium effektiv zum Einsatz zu bringen. Die Staatengemeinschaft insgesamt steht vor einer weit reichenden europäischen sowie globalen Aufgabe, die darauf zielt, die mit den neuen kommunikationstechnologischen Möglichkeiten verbundenen Chancen zwar zu nutzen, aber auch den Bürgern angesichts neuartiger Bedrohungen Schutz zu gewähren.

Dafür bedarf es der effektiven Umsetzung des Grundrechtsschutzes im nationalen und europäischen Bereich, aber auch der Fortentwicklung des Freiheitsschutzes in der globalen Dimension. Dies kann ein weiteres Überwinden territorialer Einengungen im Freiheitsschutz bedingen, der mit neuen Möglichkeiten auch des gerichtlichen Schutzes gekoppelt werden muss. Insofern können auch der Google-Entscheidung des EuGH – obwohl sie nicht direkt einschlägig ist – wichtige Anregungen für die (zumindest zukünftige) Sicherung der Durchsetzbarkeit von Rechtsschutz entnommen werden. Besonders wichtig ist auch der in dieser Entscheidung auf vielfältige Weise betonte Grundsatz, dass die weltweit tätigen Internet-Unternehmen bei ihrer Betätigung in den EU-Mitgliedstaaten den Bindungen des europäischen Rechts- und damit in Vielem mittelbar auch der nationalen Rechtsordnungen - unterworfen sind (näher oben H)

Betroffen von den neuartigen Gefährdungen sind Felder, in denen von den Staaten, der EU, aber auch der Weltgemeinschaft Kreativität für neue Lösungen und der Wille zu deren Nutzung im nationalen und internationalen Recht gefordert sind.

Die Ergebnisse des NSA-Untersuchungsausschusses werden mit hoher Wahrscheinlichkeit viele Anlässe schaffen, um sich dieser Aufgabe auch speziell aus deutscher Sicht anzunehmen. Im Interesse der freiheitlichen Demokratie ist zu hoffen, dass dies mit Nachdruck und Erfolg umgesetzt wird..