26.10.14

Schutz von Privatheit angesichts globalisierter Kommunikation

Symposium Privatheit und selbstbestimmtes Leben in der digitalen Welt

Berlin, 20. Okt. 2014

Von Wolfgang Hoffmann-Riem

Der Schutz von Privatheit ist ein wichtiges Element des Freiheitsschutzes. Freiheitsschutz aber kann mit anderen Interessen kollidieren, etwa den Interessen derer, die Informationen aus dem Privatbereich für eigene Zwecke, auch für kommerzielle Zwecke, verarbeiten wollen. Auch der Staat kann an privaten Informationen interessiert sein, etwa bei der Wahrnehmung seiner Aufgabe zur Verhinderung oder Aufklärung von Straftaten.

Bürgerinnen und Bürger, die in der Angst leben, dass sie in ihren Rechtsgütern nicht hinreichend geschützt werden, können in ihren Möglichkeiten der Ausübung von Freiheit beschränkt sein. Der Schutz von Sicherheit ist insoweit auch Freiheitsschutz. Andererseits können Maßnahmen zur Steigerung der Sicherheit ihrerseits Freiheit gefährden. Dies ist der Fall, wenn Überwachungseingriffe die Bürger hinsichtlich ihrer Bereitschaft zur Nutzung von Freiheitsrechten einschüchtern.

Der Schutz von Privatheit hat verschiedene Facetten, etwa als Schutz vor dem Eindringen in den persönlichen oder gar intimen Bereich oder vor der Manipulation eigener Kommunikationsinhalte, aber auch vor einer unerwünschten Datenverarbeitung. Welche Facetten der Privatheitsschutz im Einzelnen hat, ist heute Thema weiterer Referate. Darauf gehe ich deshalb nicht näher ein, behandele also auch nicht digitale Privatheitspraktiken. Ebenso frage ich nicht, ob in paternalistischer Weise Schutz für Privatheit auch denen gewährt werden soll, die mit ihrer Privatheit leichtfertig umgehen.

I. Zu Entwicklungen im IuK-Bereich

Meine Überlegungen konzentrieren sich auf Grundrechtsgefährdungen, die mit der Nutzung der Infrastrukturen für die digitale Information und Kommunikation einschließlich der darüber erbrachten Dienstleistungen, insbesondere im Internet, verbunden sind. Die Entwicklung in diesem Bereich verläuft rasant, so dass grundsätzlich immer nur

Schnappschüsse des jeweiligen Entwicklungsstandes möglich sind. Jedenfalls einige Stichworte will ich nennen. Dazu gehören selbstverständlich die Digitalisierung und Computerisierung der Kommunikation, damit verbunden die Globalisierung der IuK-Infrastrukturen, der Siegeszug der Social Media, die Mobilität digitaler Kommunikation, die Auslagerung von Kommunikationsinhalten auf fremde Computer (Clouds). Weitere wichtige Entwicklungen werden mit dem Schlagwort "Internet der Dinge" verbunden. Betroffen sind die Computerisierung und Distribution von Produkten und Dienstleistungen und damit die laufende computergestützte Überwachung der entsprechenden Vorgänge. Auch der häusliche und privat-berufliche Bereich ist betroffen, so etwa durch die digitale Steuerung von Heizung, Kühlschränken oder Kochgelegenheiten. Die Bequemlichkeit der Nutzer steigt ebenso wie die Möglichkeit der Sicherung weiterer Ziele, wie etwa Energieeffizienz. Da die Daten aber an externe Datenträger übermittelt und gegebenenfalls auch für andere Zwecke verwertet werden, sind damit zugleich Gefährdungen verbunden.

Die ungeheure Größe und inhaltliche Vielfalt der Daten sowie die gestiegenen Fähigkeiten zu ihrer schnellen, auch komplexe Sachverhalte erfassenden und differenzierend auswertenden, sonst schwer durchschaubare Zusammenhänge analysierenden Möglichkeiten führen zu neuen Qualitäten der Entwicklung der Informationsgesellschaft. Dafür steht das Schlagwort „Big Data“.[1] Möglich werden damit u.a. neue Qualitäten von Prognosen, Trendermittlungen und darauf aufbauenden Strategien und Kampagnen, auch zur Beeinflussungen von Werthaltungen bis hin zum Verhalten bei politischen Wahlen.

Die Veränderungen in der Kommunikationswelt haben uns viele neue Möglichkeiten individueller und kollektiver Entfaltung verschafft und Auswirkungen in fast alle gesellschaftliche Bereiche hinein bewirkt. Die auf diese Weise real gestiegenen Möglichkeiten von Freiheit sind allerdings mit Risiken neuer Art verkoppelt, darunter auch Risken für den Schutz von Privatheit, soweit die Bürger solchen Schutz wollen.

II. Zur Entwicklung des Staates zum Präventionsstaat

Seit Jahrzehnten lässt sich in Deutschland und anderswo beobachten, dass die Aufgaben des Staates im Bereich der Sicherung von Freiheit und Sicherheit einen Gestaltwandel erfahren haben. So war das Polizeirecht – in der Tradition des rechtsstaatlich geprägten preußischen Polizeiverwaltungsrechts – durch Orientierungen an konkreten, also im Einzelfall erfass- und

[1] S. statt vieler Mayer-Schönberger/Cukier, Big Data. A Revolution That Will Transform How We Live, Work, and Think, 2013

bekämpfbaren Gefahren orientiert; das Strafrecht wurde – dem Gedankengut der Aufklärung folgend – ebenfalls rechtsstaatlich begrenzt, in erster Linie durch Orientierung an schon verwirklichten Rechtsgüterverletzungen, nämlich konkreten Straftaten. Zwar gab es schon Rechtsfiguren der Vorverlagerung, etwa durch die Institute des Gefahrenverdachts, der Anscheingefahr oder des Verdachts der Straftatenbegehung. Dennoch aber kam es noch nicht zu der jetzt beobachtbaren, immer weiter reichenden Vorverlagerung des Rechtsgüterschutzes in das Vorfeld der Gefahr und in das Vorfeld des Verdachts oder gar in das Vorfeld solcher Vorfelder.

Der von mir eben erwähnte Gestaltwandel des Staates wird begrifflich durch Verweis auf den "Präventionsstaat" hervorgehoben[2]. Nicht nur die Abwehr von Gefahren, sondern schon die Verhinderung ihrer Entstehung und damit die Gefahrenverhütung werden zur zentralen Staatsaufgabe.[3] Als Mittel dazu können auch Verdachtsgewinnungseingriffe eingesetzt werden, wie etwa die Raster- oder Schleierfahndung oder die Videoüberwachung im öffentlichen Raum. Auch kann die Risikosuche auf als riskant geltende Personenkreise und Ereignisse fokussiert werden. Als Mittel der Prävention werden die vorsorgende Datensammlung (etwa in Gestalt der Vorratsdatenspeicherung[4]) ebenso wie das Abhören von Kommunikation oder das Durchkämmen von Milliarden Daten in den globalen Kommunikationsinfrastrukturen eingesetzt – mit Risiken für die Freiheitsausübung vieler, darunter auch von Personen, die in ihrem Verhalten keinen Ansatzpunkt für Gefährlichkeit gegeben haben.

III. Garantenstellungen des Staates

Die Entwicklung hin zum Präventionsstaat hat die Garantenstellung des Staates im Bereich von Freiheit und Sicherheit auch insoweit erweitert, als es um die traditionelle Aufgabe der Abwehr von Rechtsgüterverletzungen und einer darauf bezogenen Vorsorge geht. Teil der Garantenaufgabe ist es, die Bürger dabei zugleich vor Rechtsgüterverletzungen zu schützen, die von staatlichen Maßnahmen der Abwehr oder der Vorsorge vor Gefährdungen ausgehen. Die Garantenstellung hat dadurch verschiedene Stoßrichtungen bzw. führt zu

[2] Zum Präventionsstaat siehe statt vieler die Beiträge in Huster/Rudolph (Hrsg.), Vom Rechtsstaat zum Präventionsstaat (2008).
[3] Dazu siehe statt vieler *Masing*, Die Ambivalenz von Freiheit und Sicherheit, JuristenZeitung 2011, S. 753 ff.
[4] Der EuGH hat allerdings die EU-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung für europarechtswidrig erklärt, s. EuGH, Urteil vom 8. April 2014, Rs. C-293/12 und c-594/12 (Digital Rights Ireland Ltd.), so dass noch offen ist, wieweit dieses Instrument in den EU-Mitgliedstaaten weiter genutzt oder eingeführt wird. S. auch BVerfGE 125, 260 sowie Österr. Verfassungsgerichtshof, Europäische GrundrechteZeitschrift (EuGRZ) 2014, S. 429.

Dilemmasituationen. Wird im Interesse der Vorsorge gegen mögliche Gefahren oder der Abwehr von Gefahren in Kommunikationsverhältnisse eingegriffen, bedeutet dies einen Eingriff in ein Freiheitsrecht. Der Eingriff kann zugleich die Sicherheit bei der Freiheitsausübung gefährden, nämlich bei der Ausübung des Grundrechts: Enttäuscht wird die Annahme, dass der Schutz von Privatheit "sicher" sei. Hier kommt es zu einer Sicherheitsgefährdung durch Sicherheitsvorsorge – und zwar im Hinblick auf zwei unterschiedliche Typen von Sicherheit, die im Spannungsverhältnis zueinander stehen.

Dem Schutz von Freiheit dienen insbesondere Grundrechtsnormen, die –wie auch manche andere Verfassungsnormen – einen Auftrag an den Staat zur Wahrnehmung seiner Garantenstellung enthalten.

Allerdings muss im vorliegenden Kontext berücksichtigt werden, dass die empirischen Ausgangsbedingungen des Freiheitsgebrauchs sich durch die neuen Technologien verändert haben, so dass es auch Brüche geben kann, wenn Grundrechtsnormen herangezogen werden, deren Entstehungszeit weit zurückreicht, nämlich in das analoge Zeitalter. Zu den Veränderungen der Ausgangsbedingungen gehört auch die Globalisierung der Kommunikation und damit die Begrenzung von Möglichkeiten der Staatsgewalt zum Schutz seiner Bürger.

So stammt das im Bereich technologischer Kommunikationsinfrastrukturen besonders wichtige Post- und Fernmeldegeheimnis (Art. 10 GG) aus einer Zeit, in der Grundrechtsschutz im Territorialbereich des betroffenen Staates, hier Deutschland, grundsätzlich ausreichte. Dies hat sich angesichts der Internationalität und Globalität der Kommunikationsnetze verändert. Wird der Kommunikationstransport über Netze transnational oder gar global abgewickelt, droht eine (nur) territoriale Umhegung des Grundrechtsschutzes zu kurz zu greifen. Insofern gehört zur Klärung der Reichweite der Garantenstellung auch die Prüfung, ob und wieweit der Grundrechtsschutz nur dort wirksam wird, wo Beeinträchtigungen örtlich erfolgen (etwa das Ausspähen von Daten) oder ob Anknüpfungspunkt grundrechtlichen Schutzes allein oder vorrangig der Inhalt der Kommunikation ist. Dann muss Schutz auch gewährt werden, wenn ein von einem Kommunikator aus Deutschland stammender oder an einen Rezipienten in Deutschland gerichteter Kommunikationsinhalt beeinträchtigt wird, einerlei wo dies geschieht. Ich persönlich glaube, dass allein die zweite Alternative den Prämissen des Grundrechtsschutzes unter Beachtung der gegenwärtigen Kommunikationsbedingungen entspricht. Dies führt zu grundsätzlichen Fragen des Grundrechtsschutzes, die ich hier aus Zeitgründen nicht behandeln kann.

IV. Besorgnisse aus Anlass von Vermachtungen

Eine besondere Herausforderung für den Grundrechtsschutz entsteht daraus, dass viele der für die globale Kommunikation, insbesondere im Internet, maßgebenden Akteure ihren Sitz, jedenfalls den Hauptsitz, nicht in Deutschland haben und daher nicht selbstverständlich der deutschen Rechtsordnung unterworfen sind. Hinzu kommt, dass jedenfalls die großen hier tätigen Unternehmen (wie etwa Google, Facebook, Apple oder auch Amazon) über erhebliche Machtstellungen verfügen, darunter einzelne – jedenfalls Google und Facebook – über Oligopole in ihren Hauptgeschäftsfeldern. Aber nicht nur die Großen die Branche, sondern grundsätzlich alle im IT-Bereich tätigen Unternehmen ermöglichen zwar einerseits die Freiheitsausübung anderer, etwa sonstiger Unternehmen oder Privatpersonen und vermitteln dadurch großartige Chancen. Sie können die Ausübung von Freiheit aber auch beengen oder gar einschränken, etwa durch Filterung der Informationen und Begrenzung von Zugangsmöglichkeiten.

Hier stellt sich daher auch die Frage nach rechtlichem Schutz vor privatem Machteinsatz, insbesondere gegenüber Oligopolunternehmen. Wichtig ist Schutz insbesondere vor Machteinsatz, der funktional dem staatlicher Hoheitsträger nicht nur nahe kommt, sondern in seinen Möglichkeiten in vielerlei Hinsicht sogar übersteigt. Dies betrifft im hier behandelten Kontext die faktische Macht von Unternehmen des IKT-Bereichs zum Einblicken und Eindringen in Privat- und Berufssphären - und zwar ohne Geltung der für den Staat maßgebenden rechtstaatlichen Restriktionen und demokratischen Kontrollmöglichkeiten. Hinzu kommen die Potentiale der ihnen verfügbaren Kommunikationsmöglichkeiten zur Steuerung und Filterung von Kommunikation, zur Einwirkung auf Verhalten der Menschen, auf gesellschaftliche Strukturen sowie zur Beeinflussung von Trends.

Fragen danach erübrigen sich nicht schon dadurch, dass der ökonomische Markt als Regulator wirkt. Vielmehr ist – auch angesichts der oligopolistischen Vermachtung – zu fragen ob und gegebenenfalls sicherzustellen, dass der Markt auch funktionsfähig zur Gewährleistung von Freiheit ist. Dabei sind Besonderheiten von Netzwerkeffekten der Informationsgüter zu beachten, und zwar einerseits direkte Netzeffekte, aber auch indirekte Netzeffekte mit Auswirkung auf nicht selbst an den Kommunikationsbeziehungen beteiligte Dritte[5]. Von Bedeutung sind auch sogenannte Portfolio- und Konglomerateffekte, die durch die

[5] Insoweit kann hier nur pauschal auf Literatur verwiesen werden, etwa auf *Peters*, Internet-Ökonomie, 2010; *Clement/Schreiber*, Internet-Ökonomie, 2013.

zunehmende Diversifikation der Diensteanbieter im Netz in benachbarte oder weiter entfernte Tätigkeitsbereiche entstehen und zu wechselseitigen Verstärkungen von Marktpositionen führen können[6]. Darüber hinaus ist die Frage von Bedeutung, ob die Funktionsfähigkeit von Märkten nur an typischen, über Angebot und Nachfrage gesteuerten Abläufen mit dem Ziel der Sicherung des Marktmechanismus zu messen ist oder auch an anderen, für den Kommunikationsbereich spezifischen Zielwerten, darunter den Schutz von Privatheit. Wichtig ist aber auch die generelle Sicherung der Manipulationsfreiheit der Kommunikation, der Chancengerechtigkeit des Zugangs oder auch des Vertrauens in die Sicherheit der Kommunikationsvorgänge vor Beeinträchtigungen durch Dritte, aber auch der Beachtung von Schutzgütern wie Persönlichkeitsrechten durch die in diesen Märkten als Anbieter von Diensten und Verwertern der anfallenden Daten auftretenden Unternehmen.

Die zuletzt erwähnte Problematik gewinnt besondere Bedeutung daraus, dass ein Großteil der Unternehmen ihre Leistungen an die Nutzer scheinbar unentgeltlich erbringt – jedenfalls ohne finanzielle Gegenleistung. Eine besonders wichtige Gegenleistung der Nutzer besteht vielmehr in der Eröffnung des Zugangs zu den bei den Kommunikationsvorgängen anfallenden Daten, nämlich den Verbindungs-, Bewegungs- und Inhaltsdaten. Aufgrund ihrer Verwertbarkeit als Wirtschaftsgüter erhalten die Daten eine eigene ökonomische Qualität. Ihre Auswertung muss nicht auf ökonomische Zwecke (etwa für Verkaufsaktionen oder für Werbung) begrenzt werden, sondern kann z. B. auch in politischen Kontexten eingesetzt werden. Die Daten erlauben, insbesondere bei einer Kombination mit weiteren auch aus sonstigen Datenbergen stammenden Informationen, die Schaffung von Persönlichkeits- und Bewegungsprofilen, die Ermittlung von Einstellungen, die Einstufung in Nutzertypen und den Einsatz solcher Erkenntnisse für die gezielte Werbeansprache und damit die Einflussnahme auf Marktverhalten. Möglich ist auch das großräumige und in Echtzeit erfolgende Sammeln von Wissen über gesellschaftliche Entwicklungen, Erwartungen oder Befürchtungen in der Bevölkerung, über die Veränderung von Werten usw. und die Nutzung dieses Wissens zur Beeinflussung der Entwicklung

Die Nutzer selbst haben grundsätzlich keinen Einblick in die Art der Verwertung ihrer Daten und damit auch keine Möglichkeit, den ökonomischen Wert ihrer durch den Datenzugang erbrachten indirekten Gegenleistung für die Kommunikationsunternehmen einzuschätzen. Dies gelingt schon deshalb nicht, weil sie gar nicht übersehen können, wofür welche der Daten konkret eingesetzt und wie sie ökonomisch konkret weiter verwertet werden. Auch können die Nutzer die Daten-"Währung" nur sehr begrenzt durch die sonst übliche Währung,

[6] Hierzu siehe etwa Monopolkommission, Hauptgutachten XX (2012/2013), 2014, S. 63.

nämlich Geld, ersetzen und sich durch Abwägung der Vorteile und finanziellen Kosten bei den Nutzungsentscheidungen rational im Sinne der ökonomischen Theorie verhalten.

Der schnelle Aufstieg von Akteuren wie Google oder Facebook hat die Dynamik ökonomischer Prozesse in Informationsnetzwerken verdeutlicht, insbesondere die Möglichkeit des weiteren Ausbaus von Machtpositionen. Während die Internetökonomie bisher davon ausging, dass einmal errichtete Machtpositionen aufgrund der Dynamik des Internet schnell wieder verschwinden können – insofern gibt es auch viele Beispiele für anfänglich erfolgreiche, zwischenzeitlich vom Markt verschwundene Unternehmen[7] –, zeigt sich nun, dass es einzelnen Akteuren gelingt, die Machtpositionen so zu verfestigen und weiter auszubauen, dass es jedenfalls gegenwärtig keine Anhaltspunkte dafür gibt, dass es bald zu einer Korrektur – etwa bei den "Big Five" (Google, Facebook, Apple, Microsoft, Amazon) – kommen könnte oder dass – wenn eines dieser Unternehmen vom Markt verdrängt werden sollte – an seine Stelle nicht wieder ein Oligopolist tritt.

Wichtig ist auch die Feststellung, dass die im IuK-Bereich erwirtschafteten hohen Gewinne es erfolgreichen Firmen erlauben, weitere Geschäfte mit erheblicher Einflussmacht zu betreiben. Insbesondere die Großen der Branche – wie Google – sind in der Lage, andere mit internetaffinen Tätigkeiten befasste Unternehmen zu erwerben sowie crossmedial in neuen Märkten tätig zu werden.

V. Kooperation privater Machtträger mit staatlichen Instanzen

Die Machtproblematik enthält eine über den privatwirtschaftlichen Bereich hinausgehende weitere Dimension, wenn solche Unternehmen – freiwillig oder erzwungen –, bei der Gestaltung ihrer Informationsangebote dem Druck staatlicher Instanzen nachgeben oder bei der Ausspähung von Daten oder deren Auswertung mit Trägern staatlicher Macht, insbesondere Geheimdiensten, kooperieren. Unternehmen der IT-Branche sollen sogar an der Manipulation von Soft- und Hardware mitgewirkt haben, die den staatlichen Zugriff auf Daten erleichtert[8].

[7] Siehe dazu die Angaben in Monopolkommission, Hauptgutachten XX (2012/2013), 2014, S. 60 f.
[8] Angaben hierzu insbesondere in Auswertung der von *Snowden* bereitgestellten Unterlagen bei *Rosenbach/Stark*, NSA-Komplex (2014); *Greenwald*, Globale Überwachung (2014).

VI. Rechtliche Rahmensetzungen

Die transnationalen oder gar global tätigen Unternehmen unterliegen nur sehr begrenzt wirksamen rechtlichen Bindungen. Insbesondere gibt es kein globales oder transnationales Kartellrecht zur Verhinderung des Missbrauchs von Marktmacht oder zur Beschränkung von externem Wachstum (etwa durch Fusionen). Nationales und europäisches Kartellrecht kann allerdings angewandt werden, soweit in dem betroffenen Rechtsbereich Fusionen erfolgen oder Marktmacht missbräuchlich ausgenutzt wird. Solche territorial begrenzten Anwendungsmöglichkeiten taugen allerdings nicht als Mittel gegen den Aufbau oder Missbrauch globaler oligopolistischer Macht. Es ist mir unerfindlich, wieso der Bundeswirtschaftsminister hier an die hinreichende Leistungskraft deutschen oder europäischen Kartellrechts glauben kann[9].

Auch muss hinzugefügt werden, dass die Probleme der Machtbildung und das damit verbundene Risiko der Unterminierung von Grundrechtsschutz anderer selbst dann nicht bewältigt wären, wenn es ein global oder international wirkendes Kartellrecht gäbe. Kartellrecht kann vor Missbrauch von Macht im Wettbewerb schützen. Es ist aber darüber hinaus kein Regulierungsrecht zur Sicherung anderer Gemeinwohlbedarfe, wie etwa Persönlichkeitsschutz oder Manipulationsfreiheit in der Kommunikationsteilhabe.

Die Unternehmen der IuK-Branche sind allerdings zumindest den Normen des jeweiligen Sitzlandes, beispielsweise dessen Datenschutzrecht, unterworfen. Soweit sie in anderen Staaten ohne eigenen Unternehmenssitz tätig werden – etwa dort, wo die Dienste konkret genutzt werden –, können sie auch deren rechtlichen Regelungen unterworfen sein. In der Folge sind weder die Vorschriften der Europäischen Union noch die der europäischen nationalen Rechtsordnungen für die im unionalen Gebiet tätigen privaten Kommunikationsunternehmen unbeachtlich.

Dem EuGH[10] ist zu danken, dass er die Rechtsbindung auch außerhalb des Hauptsitzlandes in der Google-Entscheidung aus dem Jahr 2014 klargestellt hat. Es ist jetzt Sache der EU, aber auch der Mitgliedsstaaten, in ihren Rechtsordnungen vermehrt für geeignete Rechtsgrundlagen zu sorgen, und zwar solche, die auch der Inter- und Transnationalität der Infrastrukturen und Geschäftsmodelle der digitalen Welt gemäß sind.

Das Lob für den EuGH muss sich allerdings in Grenzen halten, da er im konkreten Anwendungsfall – es ging um das sogenannte Recht auf Vergessen-Werden – nur

[9] Siehe den Bericht "Markt und Missbrauch" der Süddeutschen Zeitung vom 17. Oktober 2014, Nr. 239, S. 19.
[10] Dazu siehe EuGH Rechtssache C-131/12, Google Spain, Urteil vom 13. Mai 2014, in: Europäische GrundrechteZeitschrift (EuGRZ) 2014, S. 320 ff.,Rn. 60

Lösungsmöglichkeiten anbietet, die insofern eine Tendenz zu neuen Risiken enthalten, als sie zur Stärkung der Filtermacht von Google führen und differenzierende Lösungen beim Datenschutz einerseits und beim Informationszugang andererseits erschweren. Konkret ging es um die Löschung von Links der Suchmaschine Google zu Informationen im Internet, die nach Auffassung der von der Information nachteilig Betroffenen gelöscht werden müssten, etwa weil sie überholt oder unrichtig seien. Google wurde unter Anwendung der EU-Datenschutzrichtlinie 95/46 verpflichtet, unter bestimmten Voraussetzungen den Nachweis in der Suchmaschine zu löschen und damit den Zugang zu der betroffenen Information (die als solche nicht gelöscht wird) zu erschweren.

Google als privates Unternehmen wurde dadurch mit schiedsähnlichen Befugnissen zur Entscheidung darüber ermächtigt, welche Informationen über seine Suchmaschine nicht mehr erreicht werden können, also für die persönliche Information von Bürgern oder für den öffentlichen Diskurs faktisch nicht mehr zugänglich sind. Allerdings bleiben sie eventuell bei Nutzung anderer Suchmaschinen oder bei direktem Zugriff auf den (häufig nicht bekannten) primären Datenträger weiter zugänglich. Der Urheber der betroffenen Information oder der am Zugang zu ihr Interessierte ist verfahrensmäßig in den Entscheidungsprozess von Google weder selbst noch durch einen neutralen Vertreter seiner Interessen eingebunden.

Die Beseitigung des Links in der Suchmaschine ist zwar keine Zensur im klassischen Sinne, angesichts der überragenden Bedeutung der Suchmaschinen von Google für das Auffinden von Informationen im Internet hat sie aber unter den gegenwärtigen Bedingungen der Kommunikationsordnung eine zensurähnliche Wirkung. Der EuGH setzt zwar voraus, dass Links nur beseitigt werden müssen, wenn die in der Richtlinie enthaltenen Voraussetzungen (Art. 12b) erfüllt sind.[11] Es gibt aber keine Sicherungen für die Einhaltung der Vorgaben. Insbesondere sind keine Rechtsmittel der Informationsanbieter gegen entsprechende Maßnahmen von Google vorgesehen, da ein Recht auf Verlinkung nicht anerkannt ist.

Ein Rechtsmittel hat allerdings derjenige, dessen Wunsch auf Löschung nicht erfüllt wird.[12] Für Google dürfte es im Interesse der Ersparnis von Aufwand und Prozessen mit den von unerwünschten Berichten Betroffenen liegen, im Zweifel die Entfernung vorzunehmen – zumal der an der Information Interessierte kein durchsetzbares Recht gegen Google auf Erhalt des Nachweises in der Suchmaschine hat. Die unmittelbar nach der EuGH-Entscheidung von Google entwickelte Praxis bestätigt Befürchtungen, dass Google in großem Maße Links

[11] EuGH (s. Fn. 9), Rn. 66 ff., 70.
[12] EuGH (s. Fn .9), Rn. 77 ff.

beseitigen würde[13]. Es entstand sogar der Eindruck, dass Google besonders großzügig mit Löschungen war, eventuell sogar mit dem unausgesprochenen Ziel, den Eingriff des EuGH in die Entscheidungspraxis von Internetunternehmen als dysfunktional zu diskreditieren.

Die hier behandelte Entscheidung ist leider auch ein Beispiel dafür, wie hilflos eine Institution wie der EuGH der Komplexität des Netzes und der Entscheidungsmacht bestimmter Akteure gegenübersteht. Das als Grundsatzentscheidung konzipierte Urteil ging auf die vielfachen Vernetzungen der Kommunikationsinhalte und –wege und damit die spezifische Funktionsweise des Internet nur oberflächlich ein und konnte deshalb keine zukunftsweisenden Lösungswege aufzeigen oder für die Zukunft offenhalten. Die unter dem Stichwort "Recht auf Vergessenwerden" geführte, die Entscheidung des EuGH durchgängig lobende öffentliche Diskussion[14] hat ihr Augenmerk nur sehr begrenzt auf den Umstand gerichtet, dass ausgerechnet ein privates machtvolles Unternehmen, vielleicht das gegenwärtig machtvollste auf dem Globus, nunmehr eine zensurähnliche Macht im Bereich öffentlicher Diskurse oder bei der öffentlichen Zugänglichkeit von Informationen erhält.

Diese Rechtsmacht wurde vom EuGH auch dadurch verstärkt, dass er als inhaltliche Orientierung für die Entscheidung über die Löschung des Link vorgegeben hat, Persönlichkeitsschutz gehe im Regelfall der Kommunikationsfreiheit vor – also eine Vorgabe, nach der im Zweifel ein Link zu beseitigen ist. Dabei hat der EuGH eine normativ durchaus umstrittene, im EU-Recht (sowie im Recht der EMRK) bisher nicht enthaltene Regel zugrunde gelegt. Über deren grundsätzliche Geltung wurde etwa zwischen dem deutschen Bundesverfassungsgericht und dem Europäischen Gerichtshof für Menschenrechte in Straßburg lange gestritten. Eine solche weitreichende abstrakte Vorrangsregel, wie der EuGH sie jetzt formuliert hat, wurde allerdings von keinem dieser beiden Gerichte anerkannt[15].

VII. Freiheitsgefährdungen durch Geheimdienste

Die Ausführungen mögen verdeutlicht haben, dass sich die Machtverhältnisse im Kommunikationsbereich mit Auswirkungen auf die Rolle des Staates oder der EU und die Entfaltung in Wirtschaft und Gesellschaft deutlich verändert haben. Dies ist seit einiger Zeit

[13] Gut drei Monate nach der Entscheidung des EuGH sind bei Google 91.000 Löschanträge (16.500 aus Deutschland) eingegangen, von denen Google etwa der Hälfte gefolgt ist. Siehe dazu die Angaben auf den Seiten 1 und 2 des Hamburger Abendblatt vom 9. September 2014, Nr. 210.
[14] Als ein Beispiel – vom datenschutzrechtlichen Standpunkt – *Caspar*, Besprechung des EuGH-Urteils vom 13. Mai 2014 in dem Verfahren C-131/12, in: PinG ("Privacy in Germany") 04.2014, S. 133 ff.
[15] S. dazu die Caroline-Rechtsprechung: BVerfGE 99, 185, 193 ff.; 120, 180, 197 ff.; EGMR EuGRZ 2012, S. 278.

bekannt. *Edwards Snowdens* Enthüllungen haben nun aber eine neue Qualität von Freiheitsgefährdungen und Asymmetrien offenbart.

Aspekte sind das weitflächige, weitgehend außerhalb nationaler Territorien erfolgende Abfangen, die Speicherung und die Auswertung der Datenströme durch Träger von Staatsgewalt wie der NSA, gekoppelt mit dem wechselseitigen Austausch oder gar Ringtausch mit Hoheitsträgern anderer Staaten. Erklärtes Ziel ist die Vorsorge gegen Gefahren, etwa solcher durch den Terrorismus oder die organisierte Kriminalität. Das „Absaugen" oder sonstige Erfassen der Daten und deren Auswertung sind aber nicht darauf begrenzt. So ist eine Nutzung auch für Zwecke der Wirtschaftsspionage sehr wahrscheinlich[16].

Die NSA geht offenbar davon aus, für ihre Auslandsaktivitäten durch amerikanisches Recht ermächtigt zu sein und keiner zusätzlichen Bindung an Rechtsordnungen der Staaten zu unterliegen, in deren Gebiet die von den Ausspähungen betroffenen Bürger wohnen oder ihnen unterworfen sind[17]. Von einer ähnlichen Grundposition scheint auch der deutsche Bundesnachrichtendienst auszugehen. Er versteht die im BND-Gesetz und im G-10 enthaltenen Vorgaben für die Auslandsaufklärung gegen Nichtdeutsche nicht dahingehend, dass er die etwa in Art. 10 des Grundgesetzes enthaltenen Vorgaben beachten müsse. Ihm reicht als Rechtsgrundlage für die Auslandsaufklärung gegen Ausländer, dass § 1 BND-Gesetz eine entsprechende Aufgabe umschreibt. Er hält es für die Auslandsaufklärung nicht für erforderlich, dass es auch – wie es im nationalen Recht unabdingbar ist – eine Norm zur Regelung der dafür einsetzbaren Befugnisse gibt[18]. Das erscheint mir unhaltbar: Es verletzt das Institut des Gesetzesvorbehalts.

Die NSA und manche andere Geheimdienste, so der britische Geheimdienst, nutzen auch Möglichkeiten des Zugriffs auf die bei IT-Unternehmen gespeicherten Meta- und Inhaltsdaten. In der Folge kommt es zu einer Kooperation zwischen politischen und militärischen Machtträgern einerseits und den Trägern ökonomischer und kommunikativer Macht im IuK-Bereich andererseits.

[16] Vgl. *Rosenbach/Stark*, Der NSA Komplex, 2014, S.206, 271
[17] Die pauschale Behauptung der NSA, sie befolge das deutsche Recht, ist ohne nachprüfbare Substanz.
[18] Dies scheint auch die Auffassung der Bundesregierung zu sein, die bei Nachfragen stereotyp zu erklären pflegt, der BND halte sich auch bei der Auslandsaufklärung an die Verfassung und das BND-Gesetz. S. statt vieler die Antwort der Bundesregierung auf eine kleine Anfrage zur Auslandsaufklärung des BND, BT-Drucks. 18/22128 v. 16.7.2014, S.3.

VIII. Objektiv-rechtlicher Grundrechtsschutz als Ausgangspunkt für besondere Schutzvorkehrungen

Auch wenn Vorkehrungen zum nationalen und europäischen Grundrechtsschutz bisher in erster Linie in territorial orientierten Dimensionen entwickelt worden sind, ist es angesichts der Internationalisierung und Globalisierung der Kommunikation an der Zeit, diese territorialen Begrenzungen zu überwinden. Darüber hinaus müssen die Konzepte des Freiheitsschutzes überdacht und gegebenenfalls korrigiert werden, insbesondere deren häufig zu starke Konzentration auf Individualrechtsschutz.

Das Bundesverfassungsgericht hat – seinerzeit unter großem öffentlichen Beifall – den Persönlichkeitsschutz beim Eintritt in das Computerzeitalter durch ein Grundrecht gesichert, das im Kern auf "informationelle Selbstbestimmung" zielt[19]. Zwar gibt es weiterhin Möglichkeiten informationeller Selbstbestimmung und Notwendigkeiten ihres Schutzes. Das Grundrecht taugt auch weiterhin zur Abwehr nationalstaatlich organisierter und deshalb durch nationales Verfassungsrecht gebändigter Eingriffe in Kommunikation. Wer aber die Kommunikationsverhältnisse insgesamt besieht, wird nur noch begrenzt Möglichkeiten für effektiven individuellen Schutz der informationellen Selbstbestimmung finden. Die Abhängigkeit von fremden Kommunikationsunternehmen, die Notwendigkeit der (weitgehenden) Unterwerfung unter deren Allgemeine Geschäftsbedingungen – die Alternative ist der Verzicht auf die Nutzung entsprechender Kommunikationsdienste – und vor allem die Intransparenz der Bereiche, in denen Daten erhoben und verwertet werden, machen individuellen Rechtsschutz jedenfalls in größerem Ausmaße praktisch wirkungslos. Zwar gibt es begrenzte Möglichkeiten zur Eigenwehr, etwa durch Verschlüsselung, aber dies ist technisch nicht einfach und es muss einkalkuliert werden, dass die Entschlüsselungstechnologien auch weiter ausgebaut werden.

Die Abhängigkeit nicht nur der persönlichen Entfaltung, sondern fast aller Bereiche der Produktion und der Dienstleistung, der Wissensgenierung sowie der Wirkungsweise einer Demokratie von einer funktionsfähigen, vor rechtswidrigen Beeinträchtigungen geschützten Kommunikationsinfrastrukturverdeutlicht, dass nicht nur Individualrechtsschutz wichtig ist, sondern auch der Schutz der Funktionsfähigkeit der Kommunikationsordnung insgesamt. Zu dieser Funktionsfähigkeit gehören die Integrität der informationstechnischen Systeme und die Möglichkeit von Vertrauen in wirkungsvolle Sicherungen vor unerlaubten Zugriffen. Dabei

[19] Siehe BVerfGE 65, 1.

müssen insbesondere Gefährdungen berücksichtigt werden, die durch die globale Dimension der IuK-Infrastrukturen sowie deren Vermachtung bedingt sind.

Aufträge oder Pflichten der Staatsorgane zur Sicherung einer solchen Funktionsfähigkeit sind Teil solcher Staatsaufgaben, die früher als Daseinsvorsorge bezeichnet wurden. Orientierungen für die Erfüllung solcher Aufgaben folgen einerseits aus grundlegenden Staatsprinzipien, aber auch aus den objektiv-rechtlichen Gehalten von Grundrechtsnormen. Dabei ist für Deutschland davon auszugehen, dass die hier maßgebenden Grundrechtsnormen durchgehend objektiv-rechtliche Schutzaufträge enthalten, zumindest Ermächtigungen zu Schutzmaßnahmen. Dies gilt für die Kommunikationsfreiheiten (Art. 5 GG), das Telekommunikationsgrundrecht (Art. 10 GG), das Wohnungsgrundrecht (Art. 13 GG), das schon erwähnte Grundrecht auf informationelle Selbstbestimmung, aber auch für weitere eventuell betroffene Grundrechte, wie die Berufs- und Eigentumsfreiheit (Art. 12, 14 GG).

Auch andere Normen enthalten Schutzaufgaben. Speziell auf die Sicherung der Funktionsfähigkeit der IuK-Infrastrukturen – und damit auf Systemschutz, nicht auf Persönlichkeitsschutz – ist Art. 87f GG bezogen: der staatliche Auftrag zur Gewährleistung "angemessener und ausreichender Dienstleistungen" im IuK-Bereich. Dazu gehört für die Kommunikationssuchenden nicht nur die Zugänglichkeit zu den Infrastrukturen und damit der über sie transportierten Kommunikation zu angemessenen Bedingungen. Ebenso wichtig und wegen der aktuellen Gefährdungen wohl noch wichtiger ist der Schutz der Integrität und Vertraulichkeit der Nutzung der entsprechenden Infrastrukturen. Eine weitere (allerdings nur begrenzt einschlägige) Norm ist Art. 91c GG (Aufbau informationstechnischer Systeme für Bund und Länder unter Einbau erforderlicher Sicherungen, etwa auch im Bereich des E-Government).

Besondere Bedeutung für die Zukunft hat das im Jahre 2008 vom BVerfG konkretisierte Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit der eigenen informationstechnischen Systeme enthalten[20]. Dieses Grundrecht ist in Ausweitung des bisherigen Schutzes aus Art. 1 Abs. 1 GG (Schutz der Menschenwürde) und Art. 2 Abs. 1 GG (Schutz der persönlichen Entfaltungsfreiheit) abgeleitet worden und nimmt daher an deren objektiv-rechtlicher Reichweite teil.

Auch wenn der vom BVerfG anerkannte grundrechtliche Schutz im Ausgangsfall um der Freiheit des individuellen Kommunikationsverhaltens willen vorgesehen ist, wird er vom Gericht als Schutz wichtiger infrastruktureller Bedingungen moderner

[20] BVerfGE 120, 274.

Telekommunikationstechniken konkretisiert, die Voraussetzung der Ausübung von Kommunikationsfreiheiten und Persönlichkeitsschutz sind.

Mit seiner Entscheidung unterstützt das Gericht die von vielen als immer bedeutsamer erkannte Notwendigkeit von Systemschutz. Diesen können einzelne Grundrechtsträger je für sich nicht leisten und die großen Kommunikationsunternehmen haben bisher nicht unter Beweis gestellt, dass sie Systemschutz umfassend, und zwar auch und speziell im Interesse der Nutzer und gegebenenfalls unter Zurückstellung der kommerziellen Interessen der Unternehmen, leisten. Hier ist die Gewährleistungsverantwortung von Trägern mit Hoheitsgewalt gefordert. Diese reicht weiter als die Erfüllung grundrechtlicher Schutzpflichten, weil es um die Erfüllung einer darüber hinaus reichenden Staatsaufgabe der Daseinsvorsorge geht.

Die im nationalen Recht enthaltenen Schutzaufträge wirken mittelbar insofern in den internationalen/globalen Bereich hinein, als sie zugleich Aufträge an die Träger nationaler Staatsgewalt – insbesondere an die Regierungen und die Parlamente – enthalten, im Rahmen des Möglichen sich für Schutz vor Freiheitsbeeinträchtigungen auch außerhalb des eigenen Territoriums einzusetzen.

Zur Einlösung von verfassungsrechtlichen Schutzaufträgen sind die Staatsorgane zum eigenständigen Handeln berechtigt und – soweit Geheimdienste in das Telekommunikationsgeheimnis des Art. 10 GG oder andere Grundrechte eingreifen – sogar verpflichtet. Dies bedeutet beispielsweise, dass die im BND-Gesetz enthaltenen Lücken der Ermächtigung des BND geschlossen werden müssen und vom BND beispielsweise Befugnisse für die Auslandsaufklärung nur unter Beachtung des Gesetzesvorbehalts aus Art. 10 GG genutzt werden dürfen. Angesichts der Geltung des Art. 10 GG für Jedermann – also auch für Ausländer – und des Fehlens einer Beschränkung des Grundrechtsschutzes auf ein Verhalten deutscher Staatsorgane im deutschen Staatsgebiet bedarf es einer gesetzlichen Grundlage auch für Freiheitseingriffe deutscher Stellen im Ausland. Bei der Schaffung gesetzlicher Grundlagen ist es allerdings nicht von vornherein ausgeschlossen, unterschiedliche Anforderungen im Hinblick auf die Inlandsaufklärung und die Auslandsaufklärung zu normieren, soweit dies durch verfassungsrechtliche vorgaben, wie den Verhältnismäßigkeitsgrundsatz, gedeckt ist.

Soweit Beeinträchtigungen durch Träger privatwirtschaftlicher oder ausländischer Macht erfolgen und nicht im Geltungsbereich der deutschen Rechtsordnung durch deutsche Schutzvorkehrungen – unter Einschluss des Strafrechts – geahndet werden können, müssen

die Schutz- und Gewährleistungsaufträge zu Bemühungen darum führen, dass Schutz auch trans- und international abgesichert wird. Das setzt ein Zusammenwirken mit anderen Staaten voraus.

Insofern ist es von Nutzen, dass Schutzaufträge auch im europa- und völkerrechtlichen Kontext bestehen. So enthalten die im Bereich der Europäischen Union geltenden Schutznormen – zumindest zum Teil – objektiv-rechtliche Gehalte. Ergänzend sind im Unionsrecht (siehe Art. 6 Abs. 2, 3 EUV) die Garantien der EMRK heranzuziehen. Im Unionsrecht selbst sind insbesondere Art. 16 Abs. 1 und Art. 18 Abs. 1 AEUV sowie Art. 1, 6, 7, 8 und 11 der EU-Grundrechtecharta[21] von Bedeutung, 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 98 AEUV). Angesichts der Bedeutung für die Verwirklichung der Grundrechte und –freiheiten in der EU sowie der Aufgabe der Förderung der europäischen Integration wirken die Schutzaufgaben auch in den Bereich der Umsetzung allgemeiner Rechtsgrundsätze des EU-Rechts hinein. So beeinflussen sie auch die Erfüllung des Auftrags zum Auf- und Ausbau transeuropäischer Netze der Telekommunikation (Art. 170 ff. AEUV).

Ergänzend und konkretisierend kann und muss die EU Schutz durch ihre eigenen Regeln bereitstellen, so etwa bei der Ausgestaltung der geplanten Datenschutz-Grundverordnung. Soweit Schutz nur durch internationale Abkommen erreichbar ist, ist auch das Bemühen um solche Abmachungen von den Schutzaufträgen des Unionsrechts erfasst, zu aktivieren etwa beim Abschluss eines Freihandelsabkommens der EU mit anderen Staaten. Die europäischen Verträge sehen im Übrigen eine wechselseitige Unterstützung von Europäischer Union und Mitgliedsstaaten bei der Erfüllung von Aufgaben vor, die sich aus den Verträgen ergeben, und zwar auch, soweit die Erfüllung dieser Aufgaben in trans- und internationalen Bezügen erfolgt.

Abschließend sei noch hinzugefügt, dass auch das Völkerrecht Schutzaufträge kennt. Einschlägig sind etwa die internationalen Menschenrechtspakte, so Art. 17 IPbpR (Recht auf Privatleben und Freiheit der Korrespondenz) und Art. 9 I IPbpR (Recht auf Meinungs- und Informationsfreiheit). Den Bürgerrechtspakten werden objektiv-rechtliche Dimensionen zugeschrieben. Allerdings gibt es Schwierigkeiten bei der Durchsetzung.

[21] In der Google-Entscheidung (Fn. hat der EuGH die Vorgaben der Datenschutzrichtlinie 95/46 dahingehend gedeutet, dass sie bewirken, die Datenschutznormen wie Art. 8 Grundrechtecharta gegen die datenverarbeitenden privaten Stellen – im konkreten Fall Google – anzuwenden. Dies ist eine der Lehre der mittelbaren Drittwirkung nahestehende Konstruktion.

IX. Gestaltungsspielräume für die Erfüllung von Schutzaufträgen

Die Staaten als Völkerrechtssubjekte, die EU-Organe und die nationalen Staatsorgane verfügen bei der Umsetzung von Schutzaufgaben allerdings über einen Gestaltungsspielraum. Angesichts des Schutzbedarfs der Freiheit der Kommunikation und des Persönlichkeitsschutzes und der großen Bedeutung der Nutzung von IuK-Infrastrukturen dürfen die deutschen und europäischen Organe grundsätzlich nicht schon die Frage des "Ob" von Schutzvorkehrungen verneinen. Bestehen bei einem Untätigbleiben erhebliche Risiken für den Grundrechtsschutz und allgemein für die Funktionsfähigkeit der informationstechnischen Systeme, kommt eine Reduzierung des politischen Gestaltungsermessens in Betracht. Diese kann dazu führen, dass die jeweils zuständigen Staatsorgane bzw. die EU-Organe verpflichtet sind, in Umsetzung des Gewährleistungsauftrags im trans- und internationalen Bereich tätig zu werden. Es bedarf weiterer Prüfung, unter welchen Voraussetzungen eine Schrumpfung des Gestaltungsermessens auch die Möglichkeit zum Individualrechtsschutz eröffnet.

Das "Wie" des Schutzes allerdings ist aufgrund des weiten Gestaltungsspielraums grundsätzlich den Hoheitsträgern überlassen – wieder mit der Möglichkeit einer Schrumpfung des Gestaltungsermessens. Es besteht aber die Pflicht, für zielführende Maßnahmen zu sorgen, also solche, die Grundrechtsschutz real ermöglichen und die Funktionsfähigkeit informationstechnischer Systeme erhalten

In einer global vernetzten Welt kann effektiver Schutz teilweise zwar auch im nationalen Bereich, zu einem erheblichen Teil aber nur auf transnationaler/globaler Ebene oder zumindest nur in transnational/global vernetzter Weise gewährleistet werden. Es bedarf daher einer Neukonzeption von Freiheitsschutz in transnationalen/globalen Dimensionen. Dies kann einen Paradigmenwechsel, ein weiteres Überwinden territorialer Einengungen im Freiheitsschutz, bedingen, der mit neuen Möglichkeiten auch des gerichtlichen Schutzes gekoppelt werden muss.

Es geht bei der rechtlichen und praktischen Ausgestaltung der IT-Infrastrukturen um gewichtige Interessen, so um wirtschaftliche Macht, um politischen Einfluss, um militärische Schlagkraft – und dabei immer wieder um das Verhältnis von Sicherheit und Freiheit. In vielen zu diesem Themenfeld getroffenen Entscheidungen hat das BVerfG die Justierung zwischen Sicherheit und Freiheit in einer von weiten Teilen der Öffentlichkeit gutgeheißenen Weise vorgenommen: durch Anerkennung der staatlichen Aufgabe der Sicherheitsvorsorge

einerseits, aber nur bei Wahrung rechtsstaatlicher Anforderungen an die Bestimmtheit und Klarheit der gesetzlichen Ermächtigung, an die Verhältnismäßigkeit des Eingriffs und an Rechtsschutz.

Betroffen davon waren Eingriffsermächtigungen für rechtsstaatlich gebundene, gerichtlich kontrollierbare und demokratischer Legitimation unterworfene Hoheitsträger. Diese Prämisse gilt für die nun anstehende weitere Aufgabe der Sicherung einer Balance zwischen unterschiedlichen Freiheitsinteressen der IT-Unternehmen und der Nutzer ihrer Dienste unter Wahrung von Sicherheitsinteressen keineswegs uneingeschränkt. Sie passt auch nicht vollständig für Maßnahmen gegen Eingriffe fremder Hoheitsträger, und zwar auch dann nicht, wenn diese nach ihrer jeweiligen Rechtsordnung rechtsstaatlichen Anforderungen und demokratischer Legitimation ausgesetzt sind, diese Anforderungen aber inhaltlich in maßgeblicher Weise von den in Deutschland oder der EU geltenden Standards abweichen.

Auch wird uns jetzt erst so richtig klar, dass die Vorstellungen über Persönlichkeitsschutz, über wirkungsvoll ausgestalteten Rechtsschutz oder über einen auch Ausländern zugestandenen Freiheitsschutz sich in den USA erheblich von dem deutschen und vielfach auch dem europäischen unterscheiden.[22]

Im transatlantischen Dialog sollte auf Harmonisierung hingearbeitet werden, die sich inhaltlich möglichst an europäischen Vorstellungen von Persönlichkeitsschutz orientiert. Die Globalisierung der Kommunikationsverhältnisse und die Globalisierung von Gefahren auch für den Persönlichkeitsschutz und den Schutz von Privatheit insbesondere fordern eine Globalisierung der Standards für Freiheitsschutz. Dies muss Teil der Aufgabe zur verstärkten trans- und internationalen Konstitutionalisierung sein.

[22] Eine grundlegende Untersuchung zum Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen nach amerikanischem Verfassungsrecht – darunter auch zu dem Abbau dieses Freiheitsschutzes in den letzten Jahrzehnten findet sich bei *Wittmann*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014. Siehe auch *Gärditz/Stuckenberg*, Vorratsdatenspeicherung à l'américaine – Zur Verfassungsmäßigkeit der Sammlung von Telefonverbindungsdaten durch die NSA, in: JuristenZeitung 2014, S. 209 ff.