Martin Kutscha

Offene Fragen zum Überwachungs-GAU

Seit nahezu einem Jahr erfahren wir immer neue Details zum Ausmaß der weltweiten geheimdienstlichen Überwachungsaktivitäten. Mittlerweile wird sogar davon ausgegangen, dass der amerikanische Geheimdienst NSA in der Lage sei, den gesamten Telefonverkehr einzelner Länder für einen Monat komplett aufzuzeichnen, um diese Daten später durchforsten zu können.

Nach zähem Ringen stellt sich nun auch das Parlament seiner Aufgabe: Die im Bundestag vertretenen Parteien verständigten sich kürzlich auf die Einrichtung eines Untersuchungsausschusses, der das Ausmaß ausländischer Überwachungsaktivitäten sowie die mögliche Beteiligung deutscher Behörden daran überprüfen soll (s. BT-Drs. 18/843). Martin Kutscha skizziert in seinem folgenden Beitrag, welche rechtlichen und politischen Fragen die NSA-Affäre noch aufwirft.

Das Fernmeldegeheimnis, schrieb der ehemalige Verfassungsrichter Jürgen Kühling bereits im „Grundrechte-Report 2003“, dürfe „man getrost als Totalverlust abschreiben, nachdem inzwischen buchstäblich jedes Telefonat abgehört wird, sei es – in geringerem Maße – durch legale Maßnahmen staatlicher Behörden, sei es – umfassend – durch fremde Geheimdienste.“[1] Was damals vielen als übertriebener Pessimismus oder als „Spökenkiekerei“[2] vorgekommen sein mag, hat sich durch die Enthüllungen Edward Snowdens im Sommer 2013 auf drastische Weise bestätigt. Danach wertet die NSA allein in Deutschland täglich rund 20 bis 60 Millionen Telefongespräche und 10 Millionen Internet-Kontakte aus.[3] Die sog. „Metadaten“ der Telekommunikation werden in großem Umfang ausgewertet. Gemeint sind damit die Informationen, wer wann mit wem per Telefon oder Computer kommuniziert hat, also nach deutschem Recht die Verkehrs- oder Verbindungsdaten. Das klingt harmlos, ist es aber keineswegs: Durch die gezielte Auswertung dieser Daten über einen längeren Zeitraum hinweg lassen sich detaillierte Persönlichkeitsprofile der jeweiligen Nutzer_innen erstellen, die Aufschluss über deren soziale Kontakte, Neigungen, politische Einstellungen, persönliche Schwächen usw. geben. „Metadaten erzählen einem absolut alles über das Leben eines Menschen“, bekannte Stewart Baker, der ehemaliger Leiter der Rechtsabteilung der NSA freimütig; „wenn man genügend Metadaten hat, braucht man die Inhalte eigentlich gar nicht.“[4]

Die Kumpanei der deutschen Dienste

Internetenthusiasten wie Sascha Lobo[5], aber auch der Berliner Datenschutzbeauftragte Alexander Dix gehen angesichts dieser Situation davon aus, dass das Internet inzwischen zu einer weltweiten Überwachungsplattform geworden ist. Die NSA hat gewissermaßen die Rolle einer weltweiten Telefon- und Kommunikationszentrale übernommen, „sie ist so etwas wie die Spinne im Netz."[6] Der US-amerikanische Geheimdienst spitzelt allerdings keineswegs allein, sondern in einer Art Überwachungsverbund mit dem britischen Geheimdienst GCHQ, kanadischen, französischen, schwedischen und spanischen Diensten, aber auch dem deutschen BND sowie dem Verfassungsschutz.[7] Unbekannt ist indessen das genaue Ausmaß der globalen „Amtshilfe", die sich diese „befreundeten" Dienste gegenseitig leisten. In diesem Punkt wäre weitere Aufklärung vonnöten – eine Aufgabe nicht zuletzt für den kommenden parlamentarischen Untersuchungsausschuss. Jedenfalls haben die Verfassungsschutzbehörden keinerlei Schritte unternommen, die Praxis des Ausspionierens der gesamten Bevölkerung einzudämmen, wie es eigentlich ihre gesetzliche Aufgabe wäre.[8] Damit zeigt sich ein weiteres Mal das Versagen dieser Behörden, nachdem deren Untauglichkeit für die Aufklärung der neonazistischen Umtriebe durch den Skandal um die „NSU"-Terrorzelle in Deutschland offensichtlich geworden ist.

Nach wie vor wird behauptet, dass die globale Überwachung der Telekommunikation zur „Bekämpfung des internationalen Terrorismus" stattfinde. Die sei nur deshalb erfolgreich, „weil Mittel und Methoden eingesetzt wurden, die die Öffentlichkeit hierzulande kritisch bewertet. Dazu zählen der Einsatz von Drohnen in für Truppen unzugänglichen Regionen Afghanistans, Pakistans, Jemens und Somalias ebenso wie das Sammeln und Auswerten von Informationen aus Internet und Mobilfunknetzen."[9] Genauere Untersuchungen in den USA haben freilich ergeben, wie wenig solche „Erfolgsmeldungen" mit der Realität gemein haben. So konstatierte der im Januar 2014 veröffentliche Bericht einer unabhängigen Regierungskommission zur Telefonüberwachung von US-amerikanischen Bürgern durch die NSA: „Wir haben bislang keinen Fall gefunden, in dem das Programm direkt dazu beigetragen hat, bislang unbekannte Pläne für einen Terroranschlag aufzudecken oder zu verhindern."[10]

Daneben wird die mangelnde Überzeugungskraft dieses Rechtfertigungsversuchs schon durch die Tatsache belegt, dass auch zahlreiche Mitglieder der Regierungen in Europa sowie Gremien der EU gezielt überwacht werden. Dass diese Stellen in den islamistischen Terrorismus verwickelt seien, haben selbst Vertreter der NSA nicht behauptet. In diesen Fällen geht es vielmehr um das Auskundschaften politischer Entscheidungsabläufe. Eine wichtige Rolle dürfte auch Wirtschaftsspionage spielen. Ob diese Überwachungspraxis nach den Versprechungen des US-Präsidenten Obama im Januar 2014 abgestellt wird, ist sehr zweifelhaft.

Sozialkontrolle im Kentaurenstaat

Aber was ist der eigentliche Grund für die elektronischen Totalausforschung der gesamten Bevölkerung? Schlüssige Antworten auf diese Frage finden sich in der Berichterstattung durch die Massenmedien kaum. Ein zentrales Ziel der Überwachung und der algorithmenbasierten Auswertung dürfte jedenfalls darin bestehen, „Prognosegrundlagen für plausible Einschätzungen darüber zu schaffen, was und wie ein bestimmter Nutzer denkt und wie er sich in bestimmten Situationen voraussichtlich verhalten wird."[11] In diesem Punkt wäre eine tiefer greifende politikwissenschaftliche Analyse gefragt, die den Wandel des Instrumentariums politischer Herrschaft in der Gegenwart zu beleuchten hätte. Zu verweisen wäre in diesem Zusammenhang auf die wachsende Kluft zwischen dem immensen Reichtum Weniger und der zunehmenden Massenarbeitslosigkeit in vielen Ländern der Welt. „Gegenwärtige Sozialkontrolle muss diesen Schub sozialer Desintegration und Ausdifferenzierung auffangen und Sicherheitsstrategien zur Verfügung stellen, die gewährleisten, dass die von sozialer Teilhabe Exkludierten nicht zu einem unbeherrschbaren Risiko werden."[12] Vor dem Hintergrund der anhaltenden ökonomischen Krisen nehmen Industriestaaten wie die USA oder Deutschland immer mehr die Gestalt von Kentauren an: Den Reichen zeigen sie ihren liberalen menschlichen Oberkörper (z.B. durch Verzicht auf hohe Besteuerung), während die verelenden Unterschichten die Pferdehufe zu spüren bekommen.[13] Der Abbau der Wohlfahrtstaatlichkeit geht einher mit der Zunahme von Überwachung und Repression, was sich je nach den politischen, ökonomischen und sozialen Bedingungen in den verschiedenen Staaten freilich unterschiedlich darstellt. Das Dogma der „Prävention", der die schrittweise Ausweitung der Überwachungs- und Kontrollbefugnisse von Polizei und Geheimdiensten angeblich geschuldet ist, findet hier ihren eigentlichen Sinn.

Datenkraken als Nutztiere der „Sicherheitsbehörden"

Es sind aber keineswegs nur staatliche Instanzen, die sich als Datenkraken betätigen. Immerhin verfügt ein Privatunternehmen wie *Facebook* mit über einer Milliarde Nutzer weltweit über einen Bestand an persönlichen Daten, von denen auch autoritäre Überwachungsstaaten nur träumen können.[14] Was liegt also aus der Sicht der verschiedenen staatlichen „Sicherheitsbehörden" näher, als sich diesen unermesslichen Datenvorrat für die eigenen Zwecke nutzbar zu machen? Tatsächlich zahlte die NSA Millionen von Dollars an Internetunternehmen wie *Google*, damit diese ihre Datensysteme mit der PRISM-Überwachungstechnologie abstimmen.[15] Nicht nur in den USA, sondern auch in Deutschland bewähren sich die privaten Datenkraken inzwischen als Nutztier der staatlichen Strafverfolgung[16], aber auch für die Geheimdienste. Auf diese Weise ist faktisch eine Art staatlich-privater Überwachungsverbund entstanden, der durch die beabsichtigte gesetzliche Regelung der Vorratsdatenspeicherung auch in Deutschland endlich die Weihen der Legalität erhalten soll.

Aber haben nicht die Unternehmen *Facebook* und *Google* an die Regierung der USA appelliert, die Ausforschung durch die NSA einzuschränken? Freilich entspringt dieser Appell keineswegs einem Engagement für die Bürgerrechte und den Schutz der Privatsphäre, sondern der Furcht vor Umsatzeinbußen infolge eines sinkenden Vertrauens des Millionenheers ihrer Kundschaft. Von dieser möglichst viele Daten („ganz freiwillig") zu erhalten und sie gezielt auswerten zu können, bildet ja gerade das Geschäftsmodell dieser Unternehmen.[17] Dass sich eben nicht nur die staatlichen „Sicherheitsbehörden", sondern auch private Unternehmen als unersättliche Datenkraken betätigen, wird auch in der Bürgerrechtsszene nicht immer hinreichend wahrgenommen.

Die Grundrechte – vom Netz genommen?

Selbst manche Kritiker und Kritikerinnen der Überwachungspraxis gehen davon aus, dass jedenfalls die US-Dienste im Rahmen des geltenden Rechts handeln. Dies ist inzwischen in den USA umstritten, wie die divergierenden Urteile verschiedener Bundesgerichte zeigen.[18] Und dass ein geheimes Verwaltungsabkommen zwischen den USA und Deutschland die Grundlage für die massive Beschränkung des grundrechtlich geschützten Telekommunikationsgeheimnisses („Fernmeldegeheimnis" in Art. 10 GG) abgeben soll,[19] widerspricht dem rechtsstaatlichen Prinzip des Vorbehalts des Gesetzes für Grundrechtseingriffe sowie dem Publizitätsgebot, wie es sich aus Art. 19 Abs. 1 GG ergibt.

Zwar sind die Geheimdienste anderer Staaten nicht an die Grundrechte des deutschen Grundgesetzes gebunden, wohl aber an internationale Menschenrechtsverträge. Zu nennen ist hier insbesondere der Internationale Pakt über bürgerliche und politische Rechte von 1966, den auch die USA unterzeichnet haben. Dessen Art. 17 verpflichtet die Staaten zum Schutz der Privatsphäre und der Korrespondenz.

Bisher gibt es zwar kein internationales Gericht, das die Einhaltung dieses Menschenrechtspaktes kontrolliert. Diese Kontrolle obliegt vielmehr dem 2006 gegründeten Menschenrechtsrat der UNO sowie einem Menschenrechtsausschuss, der nicht nur die von den einzelnen Unterzeichnerstaaten erstatteten Berichte kritisch erörtert, sondern auch mit „allgemeinen Bemerkungen" („*general comments*") den Schutzstandard der jeweiligen Menschenrechte näher bestimmt.[20] So enthält die „allgemeine Bemerkung" Nr. 16 vom 8. April 1988 zu Art. 17 des Paktes sogar eine generelle Absage an die heimliche Überwachung der Telekommunikation: „Die Überwachung mit elektronischen oder anderen Mitteln, das Abfangen telefonischer, telegraphischer oder anderer Mitteilungen, das Abhören und die Aufnahme von Gesprächen sollten verboten sein." Zur Gewährleistung des wirksamsten Schutzes des Privatlebens solle jedermann das Recht haben, „in verständlicher Form zu erfahren, ob und gegebenenfalls welche persönlichen Daten und zu welchem Zweck in automatisierten Datenbanken gespeichert werden."[21] In diesem Punkt formulierte der Ausschuss ähnliche Vorgaben für Einschränkungen des Menschenrechts wie im berühmten Volkszählungsurteil des Bundesverfassungsgerichts von 1983.

Großbritannien, dessen Geheimdienst GCHQ sich an der Globalüberwachung ebenfalls intensiv beteiligt, ist darüber hinaus an die Europäische Menschenrechtskonvention (EMRK) gebunden, deren Art. 8 ebenfalls den Schutz der Privatsphäre und der Korrespondenz festschreibt. Zu Schutzbereich und Schranken dieses Grundrechts gibt es inzwischen eine umfangreiche Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) in Straßburg. Danach muss ein Gesetz, das Eingriffe in dieses Menschenrecht zulässt, bestimmten qualitativen Anforderungen genügen: Gesetze über geheime Überwachungsmaßnahmen, so der Gerichtshof, müssen „ausreichend bestimmt gefasst sein und den Bürgern angemessene Hinweise geben, unter welchen Voraussetzungen und Umständen die Behörden befugt sind, auf solche Maßnahmen zurückzugreifen ... Außerdem verlangt das Rechtsstaatsprinzip bei von Behörden durchgeführten geheimen Überwachungsmaßnahmen angesichts der fehlenden öffentlichen Kontrolle und der Gefahr des Amtsmissbrauchs, dass das innerstaatliche Recht angemessenen Schutz vor willkürlichen Eingriffen in die Rechte des Art. 8 EMRK bietet.“[22] Es darf bezweifelt werden, dass die Überwachung durch den britischen GCHQ sowie die anderen Geheimdienste europäischer Staaten diesem menschenrechtlichen Schutzstandard entspricht.[23] Nichtregierungsorganisationen wie der Chaos Computer Club haben denn auch im Januar 2014 Individualbeschwerde beim EGMR gegen die Überwachung durch den britischen Geheimdienst eingelegt – auf das Ergebnis darf man gespannt sein.

Was die verfassungsrechtliche Situation in Deutschland anbetrifft: Zunächst ist daran zu erinnern, dass sowohl das Grundrecht auf informationelle Selbstbestimmung als auch das Telekommunikationsgeheimnis nicht nur Abwehrrechte gegenüber der deutschen Staatsgewalt darstellen, sondern auch Schutzpflichten des Staates gegenüber Eingriffen durch andere statuieren.[24] „Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf,“ gehört darüber hinaus nach der Rechtsprechung des Bundesverfassungsgerichts „zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland.“[25] Zur Begründung hätte sich das Gericht hier auf den Begriff der „*freiheitlichen* demokratischen Grundordnung“ berufen können, der immerhin den Kern unserer Verfassung ausmachen soll (von manchen Linken nach dessen Missbrauch in der Berufsverbotepraxis der 1970er Jahre allerdings zu Unrecht mit abwertendem Unterton genannt wird).[26] Kann eine Gesellschaft wirklich noch „freiheitlich“ genannt werden, in der staatlicherseits versucht wird, die gesamte Fernkommunikation zwischen den Bürgern und Bürgerinnen zu überwachen und auszuwerten? Jacob Appelbaum, ein Mitstreiter von Edward Snowden, hat deshalb Recht, dass es nicht nur um die Freiheit im Internet geht, sondern darum, „unsere Grundwerte vor einem totalitären Überwachungsstaat zu schützen, ob in der analogen oder in der digitalen Welt.“[27]

Nichts zu verbergen?

Nicht überall ist indessen das Bewusstsein ausgeprägt, dass der Schutz der Privatsphäre von essentieller Bedeutung sowohl für die Selbstbestimmung des Einzelnen als auch für das Funktionieren von Demokratie ist. „Prima leben ohne Privatsphäre", so lautet der Untertitel eines – freilich vor den Enthüllungen Snowdens erschienenen – Buches des Bloggers Christian Heller.[28] Dieser meint, der Pfad in die Post-Privacy eröffne „viele neue Freiheitsräume."[29] Wer seine Verhältnisse offen lege, „findet Leidensgenossen, mit denen er sich zu einem gemeinsamen Vorgehen zusammentun kann."[30] Zwar ist es richtig, dass die Offenbarung persönlich erlittener Diskriminierungen o. ä. zu Solidarisierungseffekten führen kann. Sie kann aber auch das Gegenteil bewirken, wie zahlreiche Berichte über „Cyber-Mobbing" belegen.[31] Während z. B. das Coming-out eines Homosexuellen in Deutschland von vielen akzeptiert wird, kann es in anderen Ländern zu schweren Nachteilen führen.

Inzwischen sind auch mehrere Fälle bekannt geworden, in denen Beschäftigte wegen kritischer Bemerkungen über ihre Arbeitgeber oder über Firmenkunden in ihrem Facebook-Korrespondenz gekündigt wurden.[32] Welche unvorhergesehenen Folgen Mitteilungen an *Facebook*-„Freunde" haben können, musste auch eine 18jährige Deutsche erfahren, die nach ihrem Abitur als Au-pair-Mädchen in die USA reisen wollte. Ihr wurde die Einreise verweigert, weil sie einen unrichtigen Einreisegrund (Besuch) angegeben hatte. Der Einreisebeamte legte der jungen Frau einen Ausdruck ihrer Facebook-Korrespondenz mit ihrem Gastvater vor, aus der sich die Absicht der (visumspflichtigen) Au-pair-Tätigkeit ergab.[33] Damit war nicht nur dieses Vorhaben gescheitert, die Betroffene muss wohl auch für die Zukunft die USA von der Liste ihrer Reiseziele streichen.

Schon diese Beispiele widerlegen das Argument, „normale" Bürger und Bürgerinnen hätten nichts zu verbergen und bräuchten sich wegen der umfassenden elektronischen Überwachung keine Sorgen zu machen. Vielmehr gehört das Recht, nicht alles gegenüber anderen Personen, Unternehmen oder staatlichen Stellen offenbaren zu müssen, zu den unabdingbaren Voraussetzungen der Persönlichkeitsentfaltung sowie des freien politischen Engagements in einer demokratischen Gesellschaft. „Ohne einen privaten, eben nicht durchleuchteten Möglichkeitsraum gibt es keine Freiheit, sondern nur ein Leben kommerziell ausgelesener Profile und staatlich erstellter Dossiers."[34]

Gegenwehr – aber wie?

Manche sind enttäuscht, dass sich gegen den Überwachungs-GAU nicht eine ebenso breite Protestbewegung regt wie gegen die Volkszählung Mitte der 1980er Jahre. Es ist allerdings fraglich, ob die Ursache hierfür in einer generellen Gleichgültigkeit gegenüber dem Schutz der eigenen Privatsphäre zu suchen ist. Sicher: Auf der einen Seite lässt sich der Drang zur exzessiven Selbstdarstellung und -entäußerung beispielsweise

in manchen zweifelhaften Fernsehformaten beobachten. Auf der anderen Seite belegen empirische Untersuchungen, dass auch Jugendliche versuchen, durch entsprechende Privacy-Einstellungen bei Facebook ihre Privatsphäre vor dem Einblick Fremder zu schützen.[35] Der kommerziellen Auswertung ihrer Daten oder dem Zugriff der Geheimdienste können sie damit allerdings nicht entgehen.

Es gibt einen wesentlichen Unterschied zwischen der 1983 beim Bundesverfassungsgericht gescheiterten und 1987 dann durchgeführten Volkszählung in der „alten" Bundesrepublik und der heutigen Massenausforschung: Bei der Volkszählung musste der Staat sich die begehrten Daten regelrecht an der Haustür abholen, was jedem Entschlossenen die Möglichkeit bot, „Nein" zu sagen und die Offenbarung seiner Daten zu verweigern.[36] Heute hingegen werden die persönlichen Daten bei jedem Telefongespräch und bei jedem Mausklick am Computer quasi „hinter dem Rücken" der Nutzer erhoben. Wenn man nicht auf die Nutzung der modernen Kommunikationsmedien verzichten will, bleiben nur zwei Abwehrmöglichkeiten, nämlich die Begrenzung der Ausforschung durch strikte internationale Datenschutzregeln oder durch Barrieren technischer Art.

Angesichts der geradezu devoten Haltung der jetzigen Bundesregierung gegenüber der Regierung der USA besteht derzeit wenig Hoffnung für den Abschluss eines Abkommens, das eine wirksame Drosselung der Überwachungsaktivitäten vorsieht – das Versprechen des US-Präsidenten, die Telefongespräche der Bundeskanzlerin künftig nicht mehr abzuhören, ist statt dessen ein billiger Trost unter „Freunden". Bei der geplanten EU-Datenschutzgrundverordnung besteht die Gefahr einer Verwässerung durch die intensive Lobbyarbeit der datenverarbeitenden Industrie.[37] Angesichts dieser Situation setzen sowohl die Datenschutzbeauftragten Deutschlands als auch die im Chaos Computer Club organisierten Netzaktivisten mehr auf technische Instrumente des Datenschutzes wie etwa kryptographische Verfahren.[38] Verwiesen wird auf die Schwierigkeiten der Geheimdienste beim „Knacken" einer guten Verschlüsselung.[39] Voraussetzung für die massenhafte Nutzung dieser Möglichkeiten ist allerdings die bisher fehlende Bereitschaft der Millionen von Nutzern und Nutzerinnen, diese Technik auch einzusetzen. Die Verschlüsselung von Kommunikationsinhalten (z.B. in E-Mails) hilft jedoch überhaupt nicht gegen die Auswertung der sog. Metadaten (die werden dennoch unverschlüsselt übertragen). Der Erfassung und Auswertung der gesamten Kommunikationsumstände entkommt man nicht so leicht.

Eine andere Option, für die z.B. der Berliner Datenschutzbeauftragte Dix plädiert, ist der Aufbau alternativer, möglichst dezentraler Netzstrukturen.[40] Auf diese Weise können die Server in Ländern mit unzureichendem Datenschutz umgangen werden, was im Hinblick auf die faktische Monopolstellung von US-Unternehmen wie *Facebook* und *Google* allerdings auf Schwierigkeiten stoßen dürfte.

Der Diskussion um die Möglichkeiten der Gegenwehr gegenüber der globalen Überwachung müssen sich jedenfalls auch die Bürgerrechtsorganisationen stellen. Den politisch Verantwortlichen sollten sie als nachdrückliche Erinnerung ins Stammbuch schreiben: „Nicht der digitale Untertan, sondern der mündige Bürger muss das zentrale Leitbild des demokratischen Rechtsstaats bleiben."[41]

MARTIN KUTSCHA Jahrgang 1948, ist Professor i.R. für Staats- und Verwaltungsrecht in Berlin und Vorstandsmitglied der Humanistischen Union; zahlreiche Veröffentlichungen insbes. zu Grundrechts- und Verfassungsfragen, u. a. „Grundrechtsschutz im Internet?“ Baden-Baden 2013 (gemeinsam mit S. Thomé) und „Die Erkenntnisse des Polyphem. Anmerkungen zum Verfassungsschutz“ in: vorgänge Nr. 197 (1/2012), S. 86 ff.

Anmerkungen:

1 Kühling, Das Ende der Privatheit, in: Müller-Heidelberg u.a. (Hrsg), Grundrechte-Report 2003, Reinbek 2003, S. 15.
2 Plattdeutsch für „Gespenster sehen“.
3 Nach Wolf, Der rechtliche Nebel der deutsch-amerikanischen „NSA-Abhöraffäre“, in: Juristenzeitung 21/2013, S. 1039 Fn. 3.
4 Zit. nach Rusbridger, Die Welt nach Snowden, in: Blätter f. dt. u. intern. Politik 12/2013, S. 37 (39).
5 Lobo, Die digitale Kränkung des Menschen, in: F.A.Z. v. 11.1.2014.
6 Dix, Grundrechtsschutz durch informationelle Gewaltenteilung, in: Roggan/Busch (Hrsg.), Das Recht in guter Verfassung? Festschrift für M. Kutscha, Baden-Baden 2013, S. 95 (103).
7 „The Guardian“ v. 1.11.2013.
8 Vgl. § 3 Abs. 1 Nr. 2 Bundesverfassungsschutzgesetz.
9 So Krause, Sicherheit vor Terrorismus braucht Aufklärung, in: Sicherheit und Frieden 4/2013, S. 236.
10 Nach „Berliner Zeitung“ v. 24.1.2014, S. 7; vgl. auch den Bericht der „Süddeutschen Zeitung“ v. 17.1.2014 über die im Auftrag der New America Foundation erstellte Untersuchung von Bergen u.a., Do NSA’s Bulk Surveillance Programs Stop Terrorists? January 2014.
11 Wolf a.a.O. (Anm. 3), S. 1039.
12 Singelnstein/Stolle, Die Sicherheitsgesellschaft, Wiesbaden 2006, S. 31.
13 Vgl. Butterwegge, Sozialstaat am Ende? In: Roggan/Busch a. a. O. (Anm. 6), S. 53 (56) und Deppe, Autoritärer Kapitalismus. Demokratie auf dem Prüfstand, Hamburg 2013, S. 54 im Anschluss an Wacquant.
14 Vgl. Englert/Hermstrüwer, Die Datenkrake als Nutztier der Strafverfolgung, in: Rechtswissenschaft 3/2013, S. 326.
15 Vgl. Wolf a.a.O. (Anm. 3), S. 1041.
16 Vgl. den Titel des eben genannten Aufsatzes von Englert/Hermstrüwer.
17 Dazu Kutscha/Thomé, Grundrechtsschutz im Internet? Baden-Baden 2013, S. 43 ff.
18 Dazu Gärditz/Stuckenberg, Vorratsdatenspeicherung á l’américaine – Zur Verfassungsmäßigkeit der Sammlung von Telefonverbindungsdaten durch die NSA, in: Juristenzeitung 5/2014, S. 209 (213 ff.).
19 Vgl. die Darstellung bei Deiseroth, Nachrichtendienstliche Überwachung durch US-Stellen in Deutschland – Rechtspolitischer Handlungsbedarf? In: Zeitschrift für Rechtspolitik 7/2013, S. 194 und bei Wolf a.a.O. (Anm. 3), S. 1042.
20 Vgl. im Einzelnen Paech/Stuby, Völkerrecht und Machtpolitik in den internationalen Beziehungen, Hamburg 2013, S. 691 f.
21 Abgedruckt in: Deutsches Institut für Menschenrechte (Hrsg.), Die „General Comments“ zu den VN-Menschenrechtsverträgen, Baden-Baden 2005, S. 68 ff.
22 EGMR, Urteil v. 2.9.2010 zur Überwachung Tatverdächtiger mittels GPS in Deutschland, in: Neue Juristische Wochenschrift 19/2011, S. 1333 (1336).

23 Vgl. Schmahl, Effektiver Rechtsschutz gegen Überwachungsmaßnahmen ausländischer Geheimdienste? In: Juristenzeitung 5/2014, S. 220 (227 f.).
24 Ausführlich dazu Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, in: Juristenzeitung 2/2014, S. 53 (56 ff.); Kutscha/Thomé a.a.O., (Anm. 17), S. 46 ff.
25 BVerfGE 125, S. 260 (324) - Vorratsdatenspeicherung
26 Der Begriff findet sich tatsächlich im Grundgesetz, so u.a. in den Art. 18 u. 21 Abs. 2.
27 Interview in „Berliner Zeitung“ v. 21./22.12.2013.
28 Heller, Post-Privacy, München 2011.
29 Heller a.a.O., S. 8.
30 Heller a.a.O., S. 135.
31 Vgl. z.B. Voskamp/Kipker, Virtueller Pranger Internet, in: Datenschutz und Datensicherheit 12/2013, S. 787.
32 Vgl. Strauß, Bruder, zur Sonne, zu Facebook? In: Müller-Heidelberg u.a. (Hrsg.), Grundrechte-Report 2013, S. 39 (41); eine solche Kündigung wurde u.a. vom LAG Hamm, Urt. v. 10.10.2012, in: Datenschutz und Datensicherheit 4/2013, S. 251 für rechtmäßig erklärt.
33 Nach Peifer, Persönlichkeitsrechte im 21. Jahrhundert – Systematik und Herausforderungen, in: Juristenzeitung 18/2013, S. 853 (856).
34 Rheinberg, Citoyens in Neuland. Über Privatheit in Zeiten des NSA-Skandals, in: Blätter f. dt. u. intern. Politik 9/2013, S. 45 (51).
35 Vgl. Kutscha/Thomé a.a.O. (Anm. 17), S. 17.
36 Vgl. Dähne/Holländer/Kutscha, Volkszählung 87 - Generalprobe für die „zweite Wende“, in: Blätter f. dt. u. intern. Politik 2/1987, S. 173 (179 ff.).
37 Vgl. Wagner, Der Entwurf einer Datenschutz-Grundverordnung der Europäischen Kommission, in: Datenschutz und Datensicherheit 9/2012, S. 676.
38 Vgl. die Entschließung der 86. Konferenz der Datenschutzbeauftragten am 1./2.10.2013 „Sichere elektronische Kommunikation gewährleisten: Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln“, in: Datenschutz und Datensicherheit 12/2013, S. 803.
39 Vgl. den Bericht über den CCC-Kongress in der „Berliner Zeitung“ v. 30.12.2013.
40 Dix a.a.O. (Anm. 6), S. 103 f.
41 So der Hamburgische Datenschutzbeauftragte Caspar auf der 86. Datenschutzkonferenz, in: Datenschutz und Datensicherheit 12/2013, S. 758.