Sonderdruck aus:

Veröffentlichungen
der Vereinigung der Deutschen Staatsrechtslehrer
Band 75

VERFASSUNG ALS ORDNUNGSKONZEPT

Franz C. Mayer, Hans Michael Heinig

Verfassung im Nationalstaat: Von der Gesamtordnung zur europäischen Teilordnung?

Lothar Michael, Ferdinand Wollenschläger

Verfassung im Allgemeinen Verwaltungsrecht: Bedeutungsverlust durch Europäisierung und Emanzipation?

Bernhard W. Wegener, Christian Seiler

Verfassung in ausgewählten Teilrechtsordnungen: Konstitutionalisierung und Gegenbewegungen – Sicherheitsrecht / Steuerrecht

Axel Tschentscher, Heike Krieger

Verfassung im Völkerrecht: Konstitutionelle Elemente jenseits des Staates?

Berichte und Diskussionen
auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer
in Speyer vom 7.–10. Oktober 2015

De Gruyter

Redaktion: Prof. Dr. Uwe Volkmann (Frankfurt am Main)

ISBN 978-3-11-044295-3
e-ISBN (PDF) 978-3-11-044325-7
e-ISBN (EPUB) 978-3-11-043521-4

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Satz: Satzstudio Borngräber, Dessau-Roßlau
Druck: Hubert & Co. GmbH & Co. KG, Göttingen
♾ Gedruckt auf säurefreiem Papier
Printed in Germany

www.degruyter.com

Dritter Beratungsgegenstand:

Verfassung in ausgewählten Teilrechtsordnungen: Konstitutionalisierung und Gegenbewegungen im Sicherheitsrecht

1. Referat von Professor Dr. *Bernhard W. Wegener*, Erlangen-Nürnberg

Inhalt

Das Sicherheitsrecht – genauer der Teil des Sicherheitsrechts auf den ich mich hier konzentrieren möchte: der sicherheitsrechtlich angeleitete staatliche Informationszugriff und Informationsgebrauch[1] – scheint als Referenzgebiet für eine Analyse der Wirkungsmacht verfassungsrechtlicher Vorgaben hervorragend geeignet.

I. Von der verfassungsrechtlichen Dystopie zur Realitätsbeschreibung

Hier trifft ein hoch ambitionierter und streckenweise pathetisch formulierter verfassungsrechtlicher Begrenzungsanspruch auf eine Gegenbewegung, die diesen Anspruch massiv unterläuft und entwertet. Die Spannungslage zwischen verfassungsrechtlichem Anspruch und praktischer wie sicherheitsrechtlicher Realität ist hier so groß wie in kaum einem anderen Rechtsgebiet.

1. Der verfassungsrechtliche Anspruch

Zur Veranschaulichung: Glaubt man dem Bundesverfassungsgericht, dann ist „eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung" mit dem vom Grundgesetz garantierten „Recht auf informationelle Selbstbestimmung [...] nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."[2]

2. Die Realität elektronischer Kommunikation und ihrer Überwachung

Angesichts dieses Anspruchs genügt eine kurze Reflektion über unser aller tatsächliche Lage um festzustellen: wir leben – nach diesen Maßstäben – in verfassungswidrigen Zuständen, in einer verfassungswidrigen Gesellschafts- und Rechtsordnung.

Spätestens seit den Enthüllungen *Edward Snowdens* über die Informationszugriffe der US-amerikanischen National Security Agency und anderer – auch deutscher – Nachrichtendienste muss jedermann klar sein, dass wir nicht mehr wissen können, wer was wann und bei welcher Gelegenheit

[1] Für eine ebensolche Konzentration vgl. *F. Becker* Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr, NVwZ 2015, 1335 ff.; für einen weiteren Ansatz *H. A. Wolff* Verfassung in ausgewählten Teilrechtsordnungen: Konstitutionalisierung und Gegenbewegungen – Sicherheitsrecht, DVBl 2015, 1076 ff.

[2] BVerfGE 65, 1 (Rn. 154) – Volkszählung; ebenso: BVerfGE 115, 166 (188, Rn. 86) – Kommunikationsverbindungsdaten.

über uns weiß. Man muss nicht mehr paranoid, sondern nurmehr realistisch sein, um als halbwegs aktiver Internetnutzer davon auszugehen, dass Unbekannte – wenn sie nur wollen – weit mehr über einen wissen können als die Allgemeinheit, oft mehr als die engste persönliche Umgebung, ja vielleicht mehr oder zumindest anderes als man selbst von sich weiß oder sich eingesteht.

Diesbezügliche Naivität kann eine sträfliche – konkret auf staatliche Bloßstellung und Strafe hinauslaufende – Nachlässigkeit in eigenen Angelegenheiten sein, wie dies etwa der ehemalige Bundestagsabgeordnete *Edathy* schmerzhaft erfahren musste.

Eine weit gefasste politische Funktionselite wird heute von den Verfassungsschutzbehörden routinemäßig darüber aufgeklärt, dass ihre elektronische Kommunikation mit hoher Wahrscheinlichkeit umfänglich mitgeschnitten und ausgewertet wird. Spätestens seit dem im Frühsommer diesen Jahres bekannt gewordenen informationstechnischen Angriff auf das Netzwerk des Deutschen Bundestages muss auch den „einfachen" Abgeordneten und ihren Mitarbeitern klar sein, wie ungeschützt ihre politische und private Kommunikation war und vermutlich immer noch ist.

Die dergestalt korrumpierte Vertraulichkeit der elektronischen Kommunikation wirkt umso dramatischer, als diese Form der Kommunikation heute praktisch unausweichlich geworden ist und sämtliche Lebensbereiche durchdringt. Die in der Debatte nicht selten mit bildungsbürgerlicher Attitüde angemahnte Selbstbeschränkung beim Gebrauch des Internets ist für die allermeisten keine realistische Option.[3] Erst recht gilt dies für die auf diese Kommunikationsformen existentiell angewiesene politische Klasse. Auch gesamtgesellschaftlich erscheint ein Verzicht auf die immensen praktischen Vorteile moderner Kommunikations- und Informationsmittel nicht diskutabel. Er wäre zudem seinerseits mit Freiheitseinschränkungen verbunden, die verfassungsrechtlich nicht zu rechtfertigen wären.

3. *Reaktionen*

In dieser Situation einer wenigstens potentiell umfassenden staatlichen[4] Überwachung macht sich mancherorts Fatalismus breit. Kritisch gesehen

---

[3] *W. Hoffmann-Riem* Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, 53 (54). Im Ansatz ähnlich *M. Pöschl* Sicherung grund- und menschenrechtlicher Standards gegenüber neuen Gefährdungen durch private und ausländische Akteure, VVDStRL 74 (2015), 405 (446), die allerdings zugleich für „Selbstdatenschutz, insb. Datenvermeidung und Datensparsamkeit" plädiert.

[4] Der mit den neuen Kommunikationsmedien einhergehende Verlust an Privatsphäre resultiert zugleich aus Informationszugriffen und -sammlungen durch Private, die hier außer Betracht bleiben müssen; näher dazu *T. Marauhn* und *M. Pöschl* Sicherung grund-

wird weniger der Verlust an Privatheit, als vielmehr umgekehrt der gegenläufige menschenrechtliche Privatheitsanspruch. Flapsig aber mit jedenfalls zeitlich passender Einordnung ließe sich sagen: Informationelle Selbstbestimmung ist sowas von 80s. Berühmt sind entsprechende Äußerungen etwa des seinerzeitigen CEO von Sun Microsystems *Scott McNealy:* „You have zero privacy anyway – Get over it."[5]

Die Konsequenz aus den hier als unabweisliche Tatsache unterstellten umfassenden Informationszugriffen zieht eine international wachsende Bewegung, die dem Leben in der „post-privacy"-Ära positives abzugewinnen versucht.[6] Informationelle Selbstbestimmung und „Privatheit" sind für sie überkommene bürgerliche Konzepte, denen unter den Bedingungen moderner Kommunikation und Datenverarbeitung die tatsächlichen Möglichkeiten ihrer Existenz abhanden gekommen sind.

In Deutschland ist diese Bewegung noch vergleichsweise klein.[7] Verbreiteter ist die alarmierte Bürgerrechtsreaktion, die nach einer den neuen technischen Möglichkeiten entsprechenden Ergänzung und Nachsteuerung der bürgerlichen Abwehrrechte gegenüber dem staatlichen Informationszugriff ruft. „Angriff auf die Freiheit" lautet der Titel einer der bekannteren der einschlägigen Streitschriften wider die staatliche Überwachung.[8] In

---

und menschenrechtlicher Standards (o. Fn. 3), VVDStRL 74 (2015), 373 (385 ff.) und 405 (430 ff.); *C. Schertz* Der Verlust der Privatsphäre in der modernen Mediengesellschaft – Ist das Individuum noch geschützt?, Vortrag im Rahmen der 56. Bitburger Gespräche 2013. Romanhaft: *D. Eggers* The Circle, 2013.

[5] Zitiert nach *P. Sprenger* in Wired, 26.1.1999, vgl. http://archive.wired.com/politics/law/news/1999/01/17538. In die gleiche Richtung scheint vielen auch die oft zitierte Aussage des seinerzeitigen Google CEO *Eric Schmidt* zu gehen: „If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." (im Interview mit *M. Bartiromo* auf CNBC am 3. Dezember 2009. The Huffington Post 7. Dezember 2009, http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html). Zur fairen Beurteilung muss erwähnt werden, dass es *Schmidt* vor allem darum ging, den Nutzern des Internets deutlich zu machen, dass Google nicht ihr „most trusted friend" sein könne, sondern vielmehr unter den Bestimmungen des US-amerikanischen „Patriot Act" u.U. verpflichtet sei, die Nutzerinformationen an staatliche Sicherheitsbehörden zu übermitteln: "But if you really need that kind of privacy, the reality is that search engines, including Google, do retain this information for some time. And [...] we're all subject, in the US, to the Patriot Act, and it is possible that that information could be made available to the authorities."

[6] Vgl. etwa: *C. Heller* Post Privacy: Prima leben ohne Privatsphäre. 2011; *M. Weber* u.a., Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut FOKUS, Post Privacy 10, https://www.oeffentliche-it.de/documents/10181/15876/Post+Privacy.

[7] Bezeichnenderweise ist das einschlägige blog der „datenschutzkritischen Spackeria", http://blog.spackeria.org/, seit 2014 eingeschlafen.

[8] *J. Zeh/I. Trojanow* Angriff auf die Freiheit: Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte, 2009; Kritisch dazu: *M. Vec* Gefangen im Datennetz,

Reaktion auf die Enthüllungen *Snowdens* forderten Schriftsteller und zigtausende Bürger Bundeskanzlerin *Angela Merkel* in einem offenen Brief zu Gegenmaßnahmen auf. Deutschland erlebe einen „historischen Angriff" auf den demokratischen Rechtsstaat, der sich auch unter Mitwirkung deutscher Sicherheitsbehörden in einen „Überwachungsstaat" verwandelt habe.[9] Eine Antwort blieb bemerkenswerter Weise bis heute aus.

4. Ursachen

a) Entgrenzte Sicherheit?

Fragt man nach den Ursachen für die zugespitzte Spannungslage zwischen dem verfassungsrechtlichen Privatheitsanspruch einerseits und dem staatlichen Informationszugriff andererseits,[10] so stößt man schnell auf die auch in der juristischen Fachliteratur breit diskutierte These der „entgrenzten Sicherheit".[11] Mit diesem hier gebrauchten Sammelbegriff werden Phänomene beschrieben wie die Ergänzung des Strafrechts um weit gefasste Vorfeldtatbestände,[12] die Auflösung des Gefahrenbegriffs,[13] die Erweiterung der Adressaten sicherheitsbehördlicher Maßnahmen, die zu Tage tretenden Grenzziehungsschwächen der Verhältnismäßigkeit,[14] neue fließende Übergänge von Repression und Prävention und

---

FAZ 15.9.2009, http://www.faz.net/aktuell/feuilleton/buecher/rezensionen/sachbuch/ilija-trojanow-juli-zeh-angriff-auf-die-freiheit-gefangen-im-datennetz-1622810.html.

[9] Der ursprünglich von dreißig Schriftstellern und knapp 70.000 Bürgern unterzeichnete Brief findet sich unter https://www.change.org/p/bundeskanzlerin-angela-merkel-angemessene-reaktion-auf-die-nsa-aff%C3%A4re.

[10] Zum sicherheitspolitischen Hintergrund etwa *O. Lepsius* Die Grenzen der präventiv-polizeilichen Telefonüberwachung, Jura 2006, 929 ff.

[11] Meist bezogen auf das Sicherheitsrecht oder einzelne seiner Elemente: *M. Thiel* Die „Entgrenzung" der Gefahrenabwehr, 2011, 473 ff.; *M. Baldus* Entgrenzungen des Sicherheitsrechts – Neue Polizeirechtsdogmatik?, Die Verwaltung 2014, 1 ff.; *U. Volkmann* Polizeirecht als Sozialtechnologie, NVwZ 2009, 216 ff.; *O. Lepsius* Freiheit und Sicherheit – ein zunehmend asymmetrisches Verhältnis, in: G.F. Schuppert u. a. (Hrsg.) Der Rechtsstaat unter Bewährungsdruck, 2010, 23 ff.; *J. Saurer* Die Ausweitung sicherheitsrechtlicher Regelungsansprüche im Kontext der Terrorismusbekämpfung, NVwZ 2005, 275 ff. Allgemeiner zu Entgrenzungen im Sicherheitsdiskurs: *M. Kötter* Subjektive Sicherheit, Autonomie und Kontrolle – Eine Analyse der jüngeren Diskurse des Sicherheitsrechts, Der Staat 43 (2004), 371 (387 ff.).

[12] Zur Strafverfolgung im Internet: *U. Sieber* Straftaten und Strafverfolgung im Internet, Gutachten zum 69. DJT, 2012. *H. Kudlich* Strafverfolgung im Internet, GA 2011, 193 ff. Aus öffentlich-rechtlicher Sicht bereits frühzeitig: *M. Germann* Gefahrenabwehr und Strafverfolgung im Internet, 2000.

[13] Grundlegend: *T. Darnstädt* Gefahrenabwehr und Gefahrenvorsorge, 1983.

[14] *O. Diggelmann* Grundrechtsschutz der Privatheit, VVDStRL 70 (2010), 50 (71 f.). *C. Gusy* Zur Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher

der immer weiter ausgebaute Präventionsanspruch,[15] die Zusammenarbeit von Polizei und Nachrichtendiensten und die Auflösung der ehemals territorialen Grenzen der sicherheitsbehördlichen Tätigkeit. Die allermeisten dieser Entgrenzungen bedingen zugleich eine Ausweitung des sicherheitsstaatlichen Zugriffs auf die private Kommunikation. Gerade die neuen sicherheitsbehördlichen Kompetenzen der Informationserhebung und Informationsverarbeitung gelten denn auch als das eigentlich entgrenzte Aufgabenfeld.[16]

Betrachtet man allein den Aufwuchs der normativen Grundlagen der staatlichen informationellen Überwachung in Deutschland, so stellt sich der Eindruck der Entgrenzung unmittelbar ein. In immer neuen Novellierungsrunden sind schon seit den sechziger Jahren des letzten Jahrhunderts die entsprechenden rechtlichen Ermächtigungen auf ein Vielfaches ihres ehemaligen Bestandes ausgebaut worden. Rückblickend erscheint es kaum glaublich, wie eng begrenzt die staatlichen Zugriffsbefugnisse auf die private Kommunikation einmal waren. Wie gerade jüngere historische Forschungen gezeigt haben,[17] darf der Blick auf die ehemals fehlenden normativen Grundlagen aber nicht den Blick auf die tatsächliche Praxis der massenhaften Kommunikationsüberwachung verstellen, die teils ohne, teils unter Überschreitung und Missachtung (verfassungs-) rechtlicher Befugnisse und Begrenzungen auch seinerzeit bereits stattfand.[18] Der Eindruck der „Entgrenzung" rührt deshalb wenigstens teilweise auch daher, dass der

---

Staats- und Verfassungsverständnisse, VVDStRL 63 (2004), 151 (176). Jenseits der sicherheitsrechtlichen Debatte auch: *G. Lübbe-Wolff* The Principle of Proportionality in the Case-Law of the German Federal Constitutional Court, Human Rights Law Journal 2014, 12 ff.

[15] Zum Ganzen eingehend: *M. Bäcker* Kriminalpräventionsrecht – Eine rechtsetzungsorientierte Studie zum Polizeirecht, zum Strafrecht und zum Strafverfahrensrecht, 2015. Pointiert und mit Recht kritisch zur Verwendung des Risikobegriffs in diesem Zusammenhang: *J. Isensee* Aussprache zu Gewährleistung von Freiheit und Sicherheit (o. Fn. 14), VVDStRL 63 (2004), 196 (197).

[16] *M. Baldus* (o. Fn. 11), Die Verwaltung 2014, 1 (2); ebenso im Befund *M. Möstl* Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, 198 ff.; *ders.* Die neue dogmatische Gestalt des Polizeirechts – Thesen zur Integration eines modernen informationellen Vorfeldrechts in das klassische rechtsstaatliche Gefahrenabwehrrecht, DVBl. 2007, 581 (584 f.); der darin aber gerade einen Beleg für die nur relative Bedeutung der Entgrenzung erkennen will.

[17] Vgl. *J. Foschepoth* Überwachtes Deutschland – Post- und Telefonüberwachung in der alten Bundesrepublik, 2012, [4]2014; *ders.* Verfassung und Wirklichkeit: Die Überwachung des Post- und Fernmeldeverkehrs in der Geschichte der Bundesrepublik Deutschland, in: H. Neuhaus Datenschutz – aktuelle Fragen und Antworten, Atzelsberger Gespräche 2014, 11 ff., http://www.university-press.fau.de/reihen/atzelsberger-gespraeche.php.

[18] Zu den unklaren rechtlichen Grundlagen und Fortwirkungen dieser Überwachungspraxis: *D. Deiseroth* Alles legal? – Zu den rechtlichen Befugnissen und Grenzen der US-Nachrichtendienste in Deutschland, DVBl. 2015, 197 (200 ff.); vgl. auch *ders.* Nachrich-

Kanon der Ermächtigungsnormen gerade in Reaktion auf die verfassungsgerichtliche Rechtsprechung zur informationellen Selbstbestimmung erheblich ausgeweitet wurde. Weil und soweit das Bundesverfassungsgericht hinreichend bestimmte, „normenklare" Befugnisse der Datenerhebung und Datenverarbeitung verlangte, wuchs die einschlägige Normenlandschaft.[19]

Ungeachtet dieser einschränkenden Betrachtungen bleibt aber eine offenbare Erweiterung der sicherheitsbehördlichen Zwecksetzungen, des Handlungsrahmens und der Mittel festzuhalten.[20]

b) Technologischer Wandel

Von ungleich größerer Relevanz ist allerdings auch hier der technologische Wandel, auf den die neue Sicherheitspolitik aufsattelt. Dieser Wandel hat eine weitreichende Digitalisierung zwischenmenschlicher Kommunikation und Interaktion mit sich gebracht und diese zudem in wenigen Transportmedien zusammengeführt. Weil und soweit diese Kommunikation über das Internet stattfindet, haben sich auch die potentiellen Zugriffspunkte für staatliche Überwachung vervielfacht. Die technischen Möglichkeiten erlauben – entsprechende Ressourcen vorausgesetzt – Praktiken wie die unter maßgeblicher Beteiligung des vormaligen NSA-Direktors *Keith Alexander* entwickelte „Heuhaufen"-Strategie, die auf eine möglichst vollständige Erfassung, Speicherung und algorithmengestützte Auswertung der globalen Kommunikation abzielen.[21] Die Geheimdienste anderer Staaten – auch Deutschlands[22] – verfolgen Strategien und Konzepte, die diesem Vorbild – nach je eigenen technischen und finanziellen Möglichkeiten

---

tendienstliche Überwachung durch US-Stellen in Deutschland – Rechtspolitischer Handlungsbedarf?, ZRP 2013, 194 ff.

[19] Vgl. dazu mit Blick auf die Nachrichtendienste: *J. Lampe* Die Schwierigkeit der Rechtfertigung nachrichtendienstlicher Tätigkeit, NStZ 2015, 361 (362). Schließlich haben auch die neuen Techniken der Kommunikation und der Überwachung eine Ergänzung der Befugnisnormen mit sich gebracht. Zu den insoweit auch weiterhin entstehenden Notwendigkeiten beispielhaft: *C. Safferling/C. Rückert* TKÜ bei Bitcoins – Heimliche Datenauswertung bei virtuellen Währungen als Telekommunikationsüberwachung iSv § 100a StPO?, MMR 2015, 788 ff. Zur Problematik einer technikinduzierten erweiternden Auslegung strafprozessualer Ermittlungsbefugnisse: *F. Roggan* Die „Technikoffenheit" von strafprozessualen Ermittlungsbefugnissen und ihre Grenzen, NJW 2015, 1995 ff.

[20] Ebenso *U. Volkmann* (o. Fn. 11), NVwZ 2009, 216 (217 ff.).

[21] Zu den verfassungsrechtlichen Rahmenbedingungen der Überwachung durch die NSA aus deutscher Perspektive: *T. Marauhn* und *M. Pöschl* Sicherung grund- und menschenrechtlicher Standards (o. Fn. 3), VVDStRL 74 (2015), 373 (390 ff.) und 405 (438 ff.).

[22] Vgl. dazu insbesondere das bei netzpolitik.org veröffentlichte BND-Konzept „Strategische Initiative Technik", wonach es um die Sicherung eines „Gleichklangs" mit den Konzeptionen der US-amerikanischen und europäischen Partner geht und „an die Stelle der Suche nach einer ‚Nadel im Heuhaufen' [...] die Suche nach den Bruchstücken dieser Nadel

abgestuft – nacheifern.[23] So wie der britische Geheimdienst die Kommunikation an den transatlantischen Brückenköpfen des Internets erfasst,[24] so spiegelt der Bundesnachrichtendienst wesentliche Teile der über den weltweit größten Internetknoten in Frankfurt laufenden Kommunikation.[25] Ähnliches gilt für die im Zuge der NSA-Affäre publik gewordene Zuarbeit des BND bei der Erfassung des satellitengestützten Telefon- und Datenverkehrs.[26] Soweit deutsche Behörden aus dieser flächenhaften Kommunikationserfassung deutsche Kommunikationsteilnehmer mit Rücksicht auf rechtliche Beschränkungen auszusortieren suchen,[27] werden entsprechende Erkenntnisse über Partnergeheimdienste zugeliefert.[28] Hinsichtlich der noch

---

getreten" sei; https://netzpolitik.org/2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/#3-Original-Dokumente.

[23] Verfassungsrechtlich bemerkenswert ist die Entwicklung in Finnland, wo sich die Regierung um eine Verfassungsänderung bemüht, die eine entsprechende Form der Vollerfassung der elektronischen Kommunikation ausdrücklich erlauben soll, vgl. dazu *J. Lavapuro* Finnish Government and the Desire to Constitutionalize Mass Surveillance: Toward Permanent State of Emergency?, VerfBlog, 2015/8/31, http://www.verfassungsblog.de/finnish-government-and-the-desire-to-constitutionalize-mass-surveillance-toward-permanent-state-of-emergency/.

[24] Eingehend zur britischen Praxis und Rechtslage: *I. Brown* Stellungnahme NSA-Untersuchungsausschuss, 2014, abrufbar unter: https://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848; vgl. auch die entsprechende Begründung und die Stellungnahmen zu der vor dem EGMR (Az. 58170/13) anhängigen Beschwerde gegen die Überwachung durch den britischen Geheimdienst, abrufbar unter https://www.privacynotprism.org.uk/news/2013/10/03/legal-challenge-to-uk-internet-surveillance/.

[25] Vgl. dazu die Anhörung des Vorstands des Betreibers ECO des DE-CIX-Knotens *K. Landefeld* v. 25.3.2015 durch den NSA-Untersuchungsausschuss des Bundestages, https://www.bundestag.de/bundestag/ausschuesse18/ua/kw13_pa_1ua/366118. Der Betreiber übte scharfe Kritik an der aus seiner Sicht zu weit gehenden Überwachungspraxis des BND, die auch deutsche Kommunikation umfänglich erfasse. Er kündigte Klage gegen die Überwachungspraxis an, vgl. http://www.zeit.de/digital/datenschutz/2015-04/de-cix-bundesverwaltungsgericht-klage-bnd-ueberwachung.

[26] Insbesondere – aber keineswegs ausschließlich – wohl durch die Anlagen im bayerischen Bad Aibling.

[27] Wie wirksam diese Bemühungen tatsächlich sind, ist wegen der Geheimhaltung der entsprechenden Tätigkeiten (vgl. dazu die ablehnenden Aussagen der Bundesregierung, BT-Drs. 17/9640, 6; BT-Drs. 17/14739, 14 ff. „mehrstufiges Verfahren") nur schwer zu beurteilen. Dass die technisch anspruchsvolle Aussonderung nicht perfekt funktioniert, zeigen einschlägige Bemerkungen im o. Fn. 22 zitierten BND-Strategiepapier: „Insbesondere die Erkennung von G-10-relevanten Internet-Verkehren muss verbessert werden, Systeme zur schnellen, unmittelbaren Steuerung der Erfassungssysteme, verbesserte Selektions- und Filtersysteme und Systeme zur Metadatenanalyse sind zu entwickeln."

[28] Zwar ist in entsprechenden Einschätzungen regelmäßig davon die Rede, ein umfassender „Ringtausch" der flächenhaft erfassten Kommunikation finde nicht statt, vgl. etwa SPD-Bundestagsfraktion, Rechtsstaat wahren – Sicherheit gewährleisten! – Erste Konse-

jenseits des Internets stattfindenden Kommunikation soll die Vorratsdatenspeicherung Lücken schließen, die mit dem Verzicht der Anbieter auf eine umfängliche Speicherung der Verbindungsdaten entstanden sind.[29] Von beträchtlicher Bedeutung sind daneben die technologischen Entwicklungen, die den Sicherheitsbehörden eine unmittelbare Beobachtung von Personen erleichtern. Eine Liste des insoweit technisch und rechtlich Machbaren lässt sich in Deutschland etwa den §§ 20 ff. des BKA-Gesetzes entnehmen, das derzeit dem Bundesverfassungsgericht zur Prüfung auf seine Verfassungsmäßigkeit vorliegt.[30]

Der technologische Wandel ist dabei aus sicherheitspolitischer Sicht ein janusköpfiger. Während er einerseits Visionen einer vollständigen Überwachung und einer entsprechend verbesserten Sicherheitslage in greifbare Nähe zu rücken scheint, schafft er andererseits einen Raum von Kommunikation und Aktion[31] für kriminelle Aktivitäten neuer Art und neuer Qualität, in dem technologisch versierte Akteure in vormals unbekannter Leichtigkeit, Schnelligkeit und Grenzfreiheit miteinander kommunizieren und inter-

---

quenzen aus dem NSA-Skandal: Eckpunkte für eine grundlegende Reform der Strategischen Fernmeldeaufklärung des BND, 16.6.2015, 6, „wonach Anhaltspunkte für einen rechtswidrigen ‚Ringtausch', also eine wechselseitige Datenübermittlung befreundeter Dienste jeweils zur Umgehung der eigenen nationalen Restriktionen, [...] bisher nicht ersichtlich" seien. Unsicherheiten werden aber auch hier deutlich, wenn zugleich (S. 3) ein entsprechendes ausdrückliches Verbot gefordert wird. Angesichts der Nachrichten über die umfassende Zulieferung von Informationen des BND an die NSA erscheinen die restriktiven Einschätzungen denn auch zumindest in dieser Richtung kaum plausibel. Unstreitig ist auch die Übermittlung von aus der strategischen Überwachung gewonnenen Einzelerkenntnissen der NSA an den BND. Der Fall der sog. „Sauerland-Gruppe" ist dafür ein von den Sicherheitsbehörden selbst oft genanntes Beispiel, zu letzterem etwa die Feststellungen der Vertreter der Regierungskoalition im Abschlussbericht zum sog. BND-Untersuchungsausschuss: BT Drs. 16/13400, 351 f.: „Erinnert sei nur an die zum Glück rechtzeitig festgenommenen Attentäter aus dem Sauerland: Ohne einen umfangreichen Informationsaustausch mit dem Ausland wäre der von ihnen geplante verheerende Sprengstoffanschlag in Deutschland wohl kaum zu verhindern gewesen."

[29] Vgl. Gesetzentwurf der Bundesregierung v. 27.5.2015 „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten", http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RegE_Hoechstspeicherfrist.html. Kritisch dazu Stellungnahme Nr. 25/2015 des Deutschen Anwalt Vereins v. 15.5.2015; vgl. auch die Stellungnahme der EU-Kommission, Mitteilung 317 – TRIS/(2015) 02810, veröffentlicht unter https://netzpolitik.org/2015/wir-veroeffentlichen-stellungnahme-der-eu-kommission-zu-vorratsdatenspeicherung-noch-viele-weitere-maengel/#doc.

[30] Zu wesentlichen Elementen der Diskussion in der mündlichen Verhandlung *D. Hipp* Karlsruher Konter, lto-online v. 11.7.2015, http://www.lto.de/recht/hintergruende/h/bverg-verhandlung-gesetzgebung-bka-ueberwachung-privatsphaere/.

[31] Zu den Herausforderungen etwa durch die Schaffung virtueller Krypto-Währungen wie den sog. „Bitcoins" und ihres Transfers in einem „peer-to-peer"-Netzwerk pseudonymisierter Nutzer: *C. Safferling/C. Rückert* (o. Fn. 19), MMR 2015, 788 ff.

agieren und sich mit Mitteln der Verschleierung und Verschlüsselung dem sicherheitsbehördlichen Zugriff zu entziehen suchen. Das Internet erscheint hier als eine Art „Wild Digital", als von Rechtlosigkeit gekennzeichneter Raum, dessen Existenz seinerseits einen verstärkten staatlichen Zugriff legitimieren kann.

II. Verfassungsgerichtliche Rahmensetzung

Angesichts des intensiven staatlichen Zugriffs auf die private Kommunikation erscheint der Ruf nach verfassungsrechtlichen Grenzsetzungen nur allzu verständlich.

1. Bundesverfassungsgericht

Entsprechende Erwartungen richten sich in Deutschland[32] in erster Linie an das Bundesverfassungsgericht. Glaubt man der sicherheitspolitischen Debatte, so ist das Gericht seiner Aufgabe des Schutzes der Privatsphäre denn auch gerecht geworden. Das Bundesverfassungsgericht gilt hier als „Champion" der bürgerlichen Freiheitsrechte, der einen überzogenen Sicherheitsanspruch von Exekutive und Legislative regelmäßig in seine verfassungsmäßigen Schranken weist.[33]

Eine genauere Analyse der Rechtsprechung des Bundesverfassungsgerichts vermittelt ein differenzierteres Bild. Zwar hat die Zahl der einschlägigen Entscheidungen seit dem Urteil zur strategischen Telekommunikationsüberwachung von 1999[34] erheblich zugenommen.[35] Vielfach hat

---

[32] In Frankreich hat der Conseil constitutionnel die erst unlängst gesetzlich erweiterten Überwachungsbefugnisse der Sicherheitsbehörden für im Wesentlichen verfassungskonform erklärt, vgl. Décision n° 2015-713 DC, v. 23.7.2015, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/decision-n-2015-713-dc-du-23-juillet-2015.144138.html, kritisch dazu *T. de Jong* Kein Grundrechtsschutz gegen Abhörgesetz in Frankreich, VerfBlog, 2015/8/18, http://www.verfassungsblog.de/kein-grundrechtsschutz-gegen-abhoergesetz-in-frankreich/.

[33] Vgl. etwa die Bewertung bei *U. Volkmann* (o. Fn. 11), NVwZ 2009, 216 (222): „mächtigste Stütze"; *O. Diggelmann* Grundrechtsschutz der Privatheit, VVDStRL 70 (2010), 50 (71 f.). „hohe Widerständigkeit"; *F. Becker* (o. Fn. 1), NVwZ 2015, 1335; vgl. auch Sondervotum der FDP-Fraktion zum sog. BND-Untersuchungsausschuss, BT Drs. 16/13400, 428. Kritisch zu dieser vom BVerfG eingenommenen Rolle: *V. Götz* § 41 Innere Sicherheit, in: H. Kube u.a. (Hrsg.) Leitgedanken des Rechts, FS Kirchhof, 2013, 457 (462 ff.).

[34] BVerfGE 100, 313 – Strategische Telekommunikationsüberwachung BND (G 10 II).

[35] Vgl. etwa BVerfGE 100, 313 – Strategische Telekommunikationsüberwachung BND (G 10 II); BVerfGE 109, 279 – Wohnraumüberwachung; BVerfGE 110, 33 – Telekommuni-

das Gericht die angegriffenen Normen auch als zumindest teilweise verfassungswidrig verworfen.[36] Die vom Bundesverfassungsgericht formulierten Grenzziehungen waren dabei aber – jedenfalls soweit sie operativ wirksam wurden – durchweg nur relativer und meist verfahrensrechtlicher Natur. Das Gericht verlangte tatbestandlich qualifizierte und hinreichend „normenklare" Ermächtigungen und Grenzziehungen,[37] es suchte Eingriffsschwellen zu definieren[38] und formulierte Richtervorbehalte[39] oder ähnliche Prüfinstrumente,[40] es forderte einen relativen Schutz des „Kernbereichs privater Lebensgestaltung"[41] und präzise Zwecksetzungen hinsichtlich der gewonnenen Informationen,[42] es setzte dem Informationsaustausch zwischen Nachrichtendiensten und anderen Sicherheitsbehörden prinzipielle und dabei wiederum relative Grenzen[43] und es reklamierte Garan-

---

kationsüberwachung nach dem Außenwirtschaftsgesetz; BVerfGE 112, 304 – GPS-Ortung; BVerfGE 113, 29 – Sicherstellung von Datenträgern; BVerfGE 113, 348 – Telekommunikationsüberwachung nach dem niedersächsischen SOG; BVerfGE 115, 166 – Sicherstellung gespeicherter Telekommunikationsdaten; BVerfGE 115, 320 – Rasterfahndung; BVerfGE 118, 168 – Abfrage von Kontostammdaten; BVerfGE 120, 274 – Online-Durchsuchung; BVerfGE 120, 378 – automatisierte Kfz-Kennzeichenerfassung; BVerfGE 124, 43 – Beschlagnahme von E-Mails; BVerfGE 125, 260 – Bevorratung von Telekommunikations-Verkehrsdaten; BVerfGE 129, 208 – strafprozessuale Telekommunikationsüberwachung; BVerfGE 130, 151 – Bevorratung und Abfrage von Telekommunikations-Bestandsdaten; BVerfGE 133, 277 – Anti-Terror-Datei. Weitere Verfahren sind derzeit anhängig, eine Entscheidung zur Novelle des BKA-Gesetzes von 2009 steht weiter aus (Az. 1 BvR 966/09, 1 BvR 1140/09).

[36] Vgl. BVerfGE 100, 313; 109, 279; 110, 33; 113, 348; 120, 274; 120, 378; 125, 260; 130, 151; 133, 277.

[37] BVerfGE 125, 260 (338, Rn. 249) – Vorratsdatenspeicherung; BVerfGE 119, 33 (51, Rn. 97) – Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz; BVerfGE 112, 304 (315, Rn. 45) – GPS-Ortung; BVerfGE 113, 348 (375, Rn. 115) – Telekommunikationsüberwachung nach dem niedersächsischen SOG.

[38] BVerfGE 115, 320 (363, Rn. 141) – Rasterfahndung II; BVerfGE 112, 304 (316, Rn. 48) – GPS-Ortung; BVerfGE 113, 29 (52 f., Rn. 106 ff.) – Sicherstellung von Datenträgern; BVerfGE 115, 166 (191, Rn. 94; 197 f., Rn. 117 f.) – Sicherstellung gespeicherter Telekommunikationsdaten; BVerfGE 118, 168 (187, Rn. 97) – Abfrage von Kontostammdaten.

[39] BVerfGE 100, 313 (390, Rn. 262) – Strategische Telekommunikationsüberwachung BND (G 10 II), BVerfGE 115, 166 (196 f., Rn. 115) – Sicherstellung gespeicherter Telekommunikationsdaten.

[40] BVerfGE 100, 313 (395 ff., Rn. 280 ff.) – Strategische Telekommunikationsüberwachung BND (G 10 II).

[41] BVerfGE 120, 274 (335, Rn. 271) – Online-Durchsuchung; BVerfGE 109, 279 (314, Rn. 122) – Wohnraumüberwachung.

[42] BVerfGE 120, 378 (427, Rn. 163) – Automatisierte Kfz-Kennzeichenerfassung; BVerfGE 124, 43 (61, Rn. 64) – Beschlagnahme von E-Mails.

[43] BVerfGE 133, 277 (369, Rn. 213) – Anti-Terror-Datei; BVerfGE 130, 151 (194 f., Rn. 152 ff.) – Bevorratung und Abfrage von Telekommunikations-Bestandsdaten.

tien für die möglichst umfängliche nachträgliche Benachrichtigung der Betroffenen.[44]

Anders als dies mitunter – auch in Staatsrechtslehrervorträgen – eingefordert worden ist, hat das Bundesverfassungsgericht sich aber nicht dazu entschließen können, absolute Tabuzonen des staatlichen Informationszugriffs zu definieren.[45] Den Wendepunkt dürfte insoweit bereits die mit 4:4 Stimmen denkbar knapp ausgegangene Tagebuchentscheidung[46] von 1989 markieren, in der das Gericht einem abwägungsfesten Verbot des staatlichen Zugriffs auf höchstpersönliche private Aufzeichnungen eine Absage erteilte.[47] Auch anderen historisch überkommenen grundrechtlichen Tabuzonen wie etwa der der eigenen Wohnung hat das Bundesverfassungsgericht immer nur einen relativen, der Abwägung mit staatlichen Sicherheitsbelangen zugänglichen Schutz zugebilligt.[48] Entgegen anders lautenden Forderungen ist dem jedenfalls im Grundsatz[49] ausdrücklich zuzustimmen. Ein absoluter informationeller Schutz der Wohnung etwa erscheint angesichts der damit einhergehenden Gefährdungen für verfassungsrechtlich hochrangige individuelle und kollektive Schutzgüter und der insoweit ausdrücklichen gegenteiligen Entscheidung des verfassungsändernden Gesetzgebers[50] verfassungsrechtlich nicht geboten.[51]

---

[44] BVerfGE 125, 260 (Rn. 240 ff) – Vorratsdatenspeicherung; 129, 208 (251, Rn. 226) – strafprozessuale Telekommunikationsüberwachung. Zu den verfassungsrechtlichen Defiziten der einschlägigen gesetzlichen Regelungen im Bereich der strategischen Telekommunikationsüberwachung: *B. Huber* Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, NJW 2013, 2572 (2574 f.).

[45] Eine solche Tabuzone stellt auch der vom Bundesverfassungsgericht sog. „absolut geschützte Kernbereich privater Lebensgestaltung" nicht dar. Zwar sollen staatliche Informationszugriffe auf diesen Kernbereich schlechthin ausgeschlossen sein und muss ein diesen Bereich erfassender Zugriff abgebrochen werden. Das Gericht definiert den Kernbereich aber ebenso wie der Gesetzgeber nicht formal, sondern – soweit überhaupt – eher materiell. Ein für die Überwachung „hinreichender Sozialbezug" soll bei allen Äußerungen bestehen, „die sich unmittelbar auf eine konkrete Straftat beziehen", BVerfGE 109, 279 (Rn. 137) – Großer Lauschangriff. Faktisch sind damit (fast) alle für die Sicherheitsbehörden interessanten Informationszugriffe möglich. Zu den im Ergebnis sehr geringen Zahlen (6) durchgeführter Wohnraumüberwachungen, vgl. Bericht der Bundesregierung gem. Art. 13 Abs. 6 S. 1 GG für das Jahr 2013, BT-Drs. 18/2495 v. 4.9.2014.

[46] BVerfGE 80, 367 – Tagebuch.

[47] Zur diesbezüglichen Bedeutung der Entscheidung eingehender *M. Nettesheim* Grundrechtsschutz der Privatheit, VVDStRL 70 (2010), 7 (20).

[48] BVerfGE, 103, 142 (151 f., Rn. 27 ff.) – Wohnungsdurchsuchung.

[49] Zweifel mögen allerdings bestehen hinsichtlich des relativ weit gefassten Kanons der Straftatbestände, die eine informationelle Überwachung des Wohnraums ermöglichen sollen.

[50] Neuregelung des Art. 13 Abs. 3–6 GG durch Gesetz v. 26.3.1998, BGBl. I, 610.

[51] Daran vermag auch der Menschenwürdegehalt des Schutzes der Wohnung im Ergebnis nichts Grundsätzliches zu ändern; so bereits BVerfGE 109, 279 (Rn. 113 ff.) – Großer

Mit einigem Recht kritisch gesehen wird dagegen der dogmatische Ausgangspunkt der Rechtsprechung des Bundesverfassungsgerichts, das von ihm selbst aus dem allgemeinen Persönlichkeitsrecht entwickelte Recht auf informationelle Selbstbestimmung.[52] In seiner eigentumsrechtlich anmutenden Konstruktion stecken zwar möglicherweise noch erhebliche Potentiale für den Ausgleich der Interessen des Einzelnen und den seine Daten kommerziell verwertenden privaten Informationsdienstleistern. Für die Grenzziehung im Bereich des staatlichen Informationszugriffs erschiene aber eine unmittelbar auf den Schutz der Privatheit abzielende Konzeption nicht nur konstruktiv überlegen, sondern auch mit Blick auf ihre potentiellen Ergebnisse und ihre europäische und internationale Anschlussfähigkeit vorzugswürdig.[53]

Problematisch erscheint die informationelle Selbstbestimmung auch deshalb, weil sie jedenfalls von ihrem konstruktiven Ausgangspunkt her kaum eine sinnvolle Unterscheidung zwischen öffentlicher und privater Sphäre erlaubt.[54] Im Gegenteil: die mit dem Konzept der informationellen Selbst-

---

Lauschangriff. Für einen solchen absoluten Schutz aber *O. Diggelmann* Grundrechtsschutz der Privatheit, VVDStRL 70 (2010), 50 (72); ähnlich auch *M. Nettesheim* Grundrechtsschutz der Privatheit, VVDStRL 70 (2010), 7 (24).

[52] Zur Kritik etwa: *G. Britz* Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des BVerfG, in: W. Hoffmann-Riem Offene Rechtswissenschaft, 2010, 561 ff. mwN.; *W. Hoffmann-Riem* Informationelle Selbstbestimmung in der Informationsgesellschaft – auf dem Wege zu einem neuen Konzept des Datenschutzes, AöR 123 (1998), 513 ff.; *T. Vesting* Das Internet und die Notwendigkeit der Transformation des Datenschutzes, in: K.-H. Ladeur (Hrsg.) Innovationsoffene Regulierung des Internets, 2003, 155 ff.; *H. P. Bull* Informationelle Selbstbestimmung – Vision oder Illusion?, 2009; *ders.* Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese? NJW 2006, 1617 ff.; *K.-H. Ladeur* Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion? DÖV 2009, 45 ff.

[53] Zwar fehlt es im Grundgesetz wie in manchen anderen Grundrechtskatalogen an einer ausdrücklichen Gewährleistung der Privatheit. Eine entsprechende Garantie ließe sich aber dem allgemeinen Persönlichkeitsrecht kaum weniger leicht entnehmen, als die der informationellen Selbstbestimmung. Das Bundesverfassungsgericht selbst hat bereits vorsichtige Schritte hin zu einer stärker an den schutzwürdigen Sphären der Privatheit orientierten Dogmatik unternommen. Neben seiner ausgebauten Rechtsprechung zum Schutz der Wohnung und der Telekommunikation ist hier insbesondere seine Entscheidung zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu nennen, vgl. BVerfGE 120, 274 – Online-Durchsuchung, vgl. dazu etwa *T. Böckenförde* Auf dem Weg zur elektronischen Privatsphäre, JZ 2008, 925 ff. Die Entscheidung verdeutlicht zugleich aber ihrerseits die dogmatische Problematik der Konzeption der informationellen Selbstbestimmung, die zu Teilergänzungen und punktuellen Neuentwicklungen nötigt, die sich mit einer umfassenden Konzeption des grundrechtlichen Schutzes der Privatheit vermeiden ließen; kritisch deshalb etwa *M. Eifert* Informationelle Selbstbestimmung im Internet – Das BVerfG und die Online-Durchsuchungen, NVwZ 2008, 521 ff.

[54] Für den Versuch einer diese Unterscheidung erlaubenden Interpretation der informationellen Selbstbestimmung vgl. *T. Böckenförde* Die Ermittlung im Netz, 2003, 466.

bestimmung verbundene Ausdehnung des Datenschutzes über den Bereich einer räumlich und sozial eng umgrenzten Privatsphäre hinaus, kann als eine zu den sicherheitsrechtlichen Entwicklungen spiegelbildliche „Entgrenzung" begriffen werden.[55] Dies hat zu nicht unerheblichen Friktionen, Überzeichnungen und fehlgehenden Erwartungen im Datenschutzrecht beigetragen. „Kein belangloses Datum",[56] das (vermeintliche?) generelle Verbot staatlicher Datenerhebung und eine grundsätzlich technikskeptische Eingriffsdogmatik können hier genannt werden. Insoweit anders als etwa der US-amerikanischen Dogmatik des „rights to privacy"[57] fehlt der informationellen Selbstbestimmung im Ansatz die im Ergebnis dann doch unausweichliche oder jedenfalls gebotene Relativierung durch den öffentlichen Raum.[58]

Während hier in der Tendenz Überzeichnungen des Datenschutzes[59] angelegt sind, kennt die Rechtsprechung des Bundesverfassungsgerichts an anderer Stelle auch bemerkenswerte Blindstellen. Gemeint ist der Umgang mit der Informationserhebung durch die Nachrichtendienste, die das Bundesverfassungsgericht traditionell mit einer nachgerade erstaunlichen Zurückhaltung und Nachsicht behandelte.

---

[55] *M. Nettesheim* Grundrechtsschutz der Privatheit, VVDStRL 70 (2010), 7 (27 f.).

[56] BVerfGE 65, 1 (45, Rn. 158) – Volkszählung; E 118, 169 (185, Rn. 88) – Kontostammdaten; E 120, 378 (399, Rn. 66) – Automatisierter KFZ-Kennzeichenabgleich. Kritisch dazu *K.-H. Ladeur* (o. Fn. 52), DÖV 2009, 45 (49) „unglückliche Formulierung".

[57] Vgl. dazu grundlegend: *S. D. Warren/L. D. Brandeis* The right to privacy, Harvard Law Review Vol. IV December 15, 1890 No. 5, übersetzt von M. Hansen/T. Weichert https://www.datenschutzzentrum.de/allgemein/20111219-Warren-Brandeis-Recht-auf-Privatheit.html. Näher dazu: *R. A. Miller* Stellungnahme NSA-Untersuchungsausschuss – Report on the Legal Situation in the United States, 2014, 20 ff., abrufbar unter: https://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848; *D. J. Glancy* The Invention of the Right to Privacy, Arizona Law Review, v. 21, n. 1, pp. 1–39 (1979). Für eine Erweiterung des US-amerikanischen Konzeptes: *A. D. Moore* Privacy Rights – Moral and Legal Foundations, 2010.

[58] Entsprechend eng sind denn auch die von den Gerichten gezogenen Grenzen des Einsatzes privater Aufzeichnungsgeräte. Für ein grundsätzliches Verwertungsverbot der Aufzeichnungen sog. Dash-Cams in KFZ wg. eines vermeintlichem Verstoßes gegen § 6b BDSG: AG München 345 C 5551/14 v. 13.8.2014, unter Berufung auf BVerfG NJW 2009, 3279. Zur Unzulässigkeit einer permanenten, verdachtslosen Überwachung des Zugangs zu einem Wohnhaus BGH NJW 1995, 1955 (1957); und zur Videoüberwachung in der Tiefgarage einer Wohnungseigentumsgemeinschaft LG München I, Urteil vom 11. 11. 2011, Az. 1 S 12752/11.

[59] Kritisch zum Volkszählungsurteil als der „Bergpredigt des Datenschutzrechts": *K. v. Lewinski* Staat als Zensurhelfer – Staatliche Flanierung der Löschpflichten Privater nach dem Google-Urteil des EuGH, AfP 2015, 1, 3. Eingehender: *H. P. Bull* Sinn und Unsinn des Datenschutzes – Persönlichkeitsschutz und Kommunikationsfreiheit in der digitalen Gesellschaft, 2015.

2. *Europäische Verfassungsgerichte*

Eine zunehmende Rolle bei der verfassungsrechtlichen Grenzsetzung der sicherheitsbehördlichen Überwachung werden künftig die europäischen Verfassungsgerichte, der Gerichtshof der Europäischen Union (EuGH) und der Europäische Gerichtshof für Menschenrechte (EGMR)[60] spielen. Dafür spricht einerseits die technische Tatsache der alltäglich weltumspannenden Kommunikation, die nach übernationalen[61] Antworten verlangt. Dafür spricht andererseits der Umstand, dass die Europäische Union ihrerseits erhebliche Anstrengungen unternimmt, um das Spannungsverhältnis von Datenschutz und Sicherheitsrecht normativ zu gestalten.[62]

---

[60] Auch der EGMR ist normativ gut gerüstet für die Aufgabe der Freiheitssicherung gegenüber den Sicherheitsbehörden. Die Europäische Menschenrechtskonvention enthält in Art. 8 ebenso wie die EU-Grundrechtecharta eine ausdrückliche Garantie des Privatlebens, der Wohnung und der Korrespondenz. Auch hat der EGMR diese Garantien in seiner Rechtsprechung schon früh und durchaus wirkmächtig entfaltet, vgl. den Rechtsprechungsüberblick bei *S. Schiedermair* Der Schutz des Privaten als internationales Grundrecht, 2012, 422 ff.; weitere Rechtsprechung bei *U. Karpenstein/F. C. Mayer* EMRK, 2015, Art. 8, Rn. 61 ff. Zum Schutzbereich: *C. Grabenwarter/K. Pabel* Europäische Menschenrechtskonvention, 2012, 240 f. Gerade für Deutschland wird seine Funktion sich aber aller Voraussicht nach entsprechend dem Charakter der Konvention und angesichts des hier relativ stark ausgebauten nationalen und supranationalen Grundrechtsschutzes auf die Korrektur einzelner Fehlentwicklungen beschränken; für eine entspr. Einschätzung der deutschen Rechtslage insbesondere: EGMR, Az. 54934/00, 29.6.2006 – Weber und Saravia/D. Dafür spricht auch der Umstand, dass es dem EGMR als reinem Menschenrechtsgerichtshof an einer einfachgesetzlichen Grundlage für die vielfach technischen und komplexen Detailfragen des sicherheitsbehördlichen Informationszugriffs und des Datenschutzes fehlt. Zu der aktuell beim EGMR (Az. 58170/13) anhängigen Beschwerde gegen die Internetüberwachung durch den britischen Geheimdienst bereits o. Fn. 24. Zur Rechtsprechung des EGMR gerade im Hinblick auf die Überwachungspraxis der Geheimdienste: vgl. EGMR, Az. 47143/06, 4.12.2015 – Sacharow v. Russland; EGMR, Az. 37138/14, 12.1.2016 – Szabó und Vissy v. Ungarn; sowie *D. Korff* Stellungnahme NSA-Untersuchungsausschuss, 2014, 14 ff.; abrufbar unter: https://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848.

[61] Der Sache nach ist hier eine globale Regulierung angezeigt, die sich jenseits der Fragen technischer Normung aber erst in Ansätzen erkennen lässt. Vgl. insoweit etwa UN-General Assembly Resolution 68/167, 12/2013 on the right to privacy in the digital age. Dazu auch Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, 30.6.2014, A/HRC/27/37; *W. Hoffmann-Riem* (o. Fn. 3), JZ 2014, 53 ff.; *H. P. Aust* Sachverständigengutachten über völker- und europarechtliche Fragen der Erhebung, Speicherung und Verarbeitung von Daten, Skeptisch zu entsprechenden Bestrebungen der Bundesregierung *M. Kotzur* Datenschutz als Menschenrecht?, ZRP 2015, 216 ff.

[62] Vgl. dazu die Vorschläge der EU-Kommission v. 25.1.2012 für eine neue EU-Datenschutz-Grundverordnung, KOM (2012) 11 endg. und für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von

Insbesondere der EuGH sieht sich denn auch mit erheblichen Erwartungen an eine möglichst freiheitssichernde Rechtsprechung konfrontiert. Mit der im internationalen Vergleich immer noch seltenen textlichen Grundlage einer ausdrücklichen doppelten grundrechtlichen Garantie des Schutzes des Privatlebens und der personenbezogenen Daten scheint er dafür gut gerüstet. Außerdem sollte nicht übersehen werden, dass die Europäische Union als solche derzeit noch so gut wie keine eigenen Polizei- und Strafverfolgungsbehörden sowie Nachrichtendienste unterhält; entsprechende Rücksichtnahmen von Seiten des Gerichtshofs liegen also nicht unbedingt nahe. So könnte etwa die soeben ergangene Entscheidung zu dem wegen der NSA-Zugriffe für nicht hinreichend sicher erklärten Datenaustausch mit den USA einschneidende Wirkungen entfalten.[63] Schon die erste große einschlägige Grundentscheidung,[64] mit der der Gerichtshof die EU-Richtlinie über die Vorratsdatenspeicherung als unverhältnismäßigen Grundrechtseingriff in Gänze verworfen hat, hat bei Datenschützern ein euphorisches Echo[65] gefunden.[66] Auch in der rechtswissenschaftlichen Diskussion wird der EuGH ange-

---

Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM (2012) 10 endg. Dazu aus dem laufenden Gesetzgebungsverfahren: legislative Entschließung des Europäischen Parlaments vom 12.3.2014 zur Datenschutz-Grundverordnung, P7_TA (2014)0212; und Vorbereitung einer allgemeinen Ausrichtung, Ratsdokument 9565/15, 11.6.2015. Zu einer kritischen Einschätzung der Vorschläge aus datenschützerischer Sicht: Stellungnahme 3/2015 des Europäischen Datenschutzbeauftragten, Eine große Chance für Europa, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_DE.pdf; vgl. auch die rechtlich eingehendere ältere Stellungnahme: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_DE.pdf. Vgl. auch *J. Kühling* Europäisierung des Datenschutzrechts – Gefährdung deutscher Grundrechtsstandards?, 2014. Insbesondere für die im Folgenden im Vordergrund stehenden Fragen der geheimdienstlichen Überwachung darf allerdings nicht übersehen werden, dass schon das EU-Primärrecht in Art. 4 Abs. 2 S. 3 EUV und Art. 73 AEUV einen grundsätzlichen mitgliedstaatlichen Kompetenzvorbehalt für Aufgaben der „nationalen Sicherheit" kennt. Diese Beschränkung setzt sich in den aktuell diskutierten Vorschlägen zur Sekundärrechtssetzung in nicht immer deutlicher Form fort.

[63] EuGH, Rs. C-362/14, Urt. v. 6.10.2015 – Schrems; vgl. dazu auch Schlussanträge des GA *Y. Bot* v. 23.9.2015. Eingehender zur Problematik: *J. Rauhofer/C. Bowden* Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud (June 21, 2013). Edinburgh School of Law Research Paper No. 2013/28, abrufbar unter: http://ssrn.com/abstract=2283175 oder http://dx.doi.org/10.2139/ssrn.2283175.

[64] Vgl. im Übrigen den Überblick zur älteren Rechtsprechung der EU-Gerichte zum Schutz der Privatheit bei *S. Schiedermair* (o. Fn. 60), 2012, 438 ff.

[65] Vgl. etwa *A. Roßnagel* MMR 2014, 372, 377 mwN auf die publizistischen und politischen Einschätzungen, die sich zwischen einer Einordnung als „Magna Charta für den Datenschutz" und einem „Feiertag für das organisierte Verbrechen" bewegen.

[66] EuGH, verb. Rs. C-293, 594/12, 8.4.2014 – Digital Rights Ireland.

sichts dieser Entscheidung als neuer Verteidiger bürgerlicher Freiheiten gefeiert, der über die entsprechenden Vorgaben des Bundesverfassungsgerichts – das seinerseits eine begrenzte Vorratsdatenspeicherung ausdrücklich für mit dem Grundgesetz vereinbar erklärt hatte – noch deutlich hinausgegangen sei.

Eine nähere Betrachtung beider Urteile offenbart aber erhebliche Begründungsschwächen.

So mag man der Facebook-Entscheidung im Ergebnis zustimmen. Wegen der Informationszugriffe der NSA und anderer US-amerikanischer Behörden können die USA nicht als sicherer Datenhafen bewertet werden. Angesichts der weder durch das EU-Recht noch durch das Recht der meisten Mitgliedstaaten wirksam begrenzten Informationszugriffe europäischer Nachrichtendienste vermag der Hinweis auf das angeblich bessere EU-Datenschutzniveau aber kaum zu überzeugen.

Die Entscheidung zur Richtlinie über die Vorratsdatenspeicherung erscheint mir darüber hinaus auch im Ergebnis nicht überzeugend. Zwar rügte der EuGH vordergründig lediglich, dass die EU-Richtlinie über die Vorratsdatenspeicherung keine einschränkenden tatbestandlichen Voraussetzungen, keine Straftatenkataloge, keine hinreichend restriktiv definierten Speicherungszeiträume, keine richterlichen Vorbehalte und damit insgesamt „keine klaren und präzisen Regeln" zur Tragweite der Eingriffe in Art. 7 und 8 der EU-Grundrechtecharta vorsah.[67] Das Fehlen entsprechender Regelungen hätte ein entsprechendes deutsches Gesetz auch vor dem Bundesverfassungsgericht zu Fall gebracht. Irritierend erscheint jedoch, mit welcher Selbstverständlichkeit der EuGH aus den Grundrechten eine Verpflichtung zu einer solchen Ausgestaltung auch einer EU-Richtlinie verlangt. Gegen solche Ausgestaltungserfordernisse spricht die Natur der Richtlinie[68] als einer jedenfalls potentiell bloßen Rahmengesetzgebung, die den Mitgliedstaaten lediglich Ziele vorgibt, ihnen aber die Wahl der Form und der Mittel und damit auch die Ausgestaltung im einzelnen überlassen kann. Unter der Hand mutiert hier der Grundrechtsschutz zu einer Vollregelungsverpflichtung, die sich mit der Grundregel der begrenzten, geteilten und subsidiären EU-Kompetenz nicht vereinbaren lässt. Diese Rechtspre-

[67] EuGH, verb. Rs. C-293, 594/12, 8.4.2014 – Digital Rights Ireland, Rn. 65.

[68] In der Sache ändert sich an der kompetenzrechtlichen Problematik auch dann nichts, wenn die EU – wie derzeit für die neue Datenschutz-Grundverordnung vorgesehen – vom Regelungsinstrument der Richtlinie zu dem der Verordnung wechselt. Zwar ist mit diesem Regelungsinstrument dem Charakter nach eine Vollharmonisierung möglich. Der konkrete Vorschlag ist davon aber mit Rücksicht auf die hoch verschiedenen mitgliedstaatlichen Regelungsansätze und -traditionen zu Recht weit entfernt. Eine weitere Harmonisierung soll erst durch eine weitere Konkretisierung der Grundverordnung im sog. „Kohärenzverfahren" erreicht werden.

chung hat – sollte sie auf die anstehende neue EU-Datenschutzgesetzgebung und auf andere Regelungsbereiche übertragen werden – das Potential, weit größere als die schon in der Vergangenheit beobachteten Kompetenzverschiebungen zu Lasten der Mitgliedstaaten mit sich zu bringen.[69]

III. Neue verfassungsrechtliche Grenzsteine

Angesichts der jedenfalls in vielen Ergebnissen[70] überzeugenden verfassungsgerichtlichen Rahmensetzung kann es im Folgenden nicht um eine grundsätzliche verfassungsrechtliche Neubestimmung staatlichen Informationszugriffs und Informationsgebrauchs gehen. Notwendig erscheinen eher evolutionäre Korrekturen und Ergänzungen.

1. Verfassung als Rahmenordnung

Ausgangspunkt muss dabei das Verständnis der Verfassung als einer Rahmenordnung sein. Gerade Fragen des Ausgleichs von Freiheit und Sicherheit sind der Sache nach regelmäßig politischer Natur und damit weithin dem demokratischen Entscheidungsprozess überantwortet.[71] Die spezifisch deutsche Sensibilität für den Datenschutz gibt Anlass, dies zu betonen und vor aus der historischen Erfahrung abgeleiteten Übertreibun-

---

[69] *U. Haltern* Das Machtspiel der Gerichte, NZZ Nr. 175, v. 31.7.2014; *M. Ruffert* Schlüsselfragen der europäischen Verfassung der Zukunft, EuR 2004, 165 (169 ff.); *J. Kühling* Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung, Die Verwaltung, 2007, 153 ff.

[70] Die dogmatische Sicherheit des Bundesverfassungsgerichts wird dagegen in der sicherheitsrechtlichen Literatur vielfach skeptisch gesehen, vgl. etwa *M. Baldus* (o. Fn. 11), Die Verwaltung 2014, 1 (15) „Unsicherheiten und Schwächen der Rechtsprechung angesichts der Entgrenzungsvorgänge verfassungsrechtliche Grenzlinien zu bestimmen".

[71] Vgl. SächsVerfGH, LKV 1996, 273, 280; *M. Thiel* Die „Entgrenzung" der Gefahrenabwehr, 2011, 184; *H.-H. Trute* Grenzen des präventionsorientierten Polizeirechts in der Rechtsprechung des Bundesverfassungsgerichts, Die Verwaltung, Bd. 42 (2009) 85 (87 f.); *F. Schoch* Abschied vom Polizeirecht des liberalen Rechtsstaats? – Vom Kreuzberg-Urteil des Preußischen Oberverwaltungsgerichts zu den Terrorismusbekämpfungsgesetzen unserer Tage, Der Staat Bd. 43 (2004) 347 (367). Zu den Grenzen, BVerfGE 115, 320 (360) – Rasterfahndung: „Die Balance zwischen Freiheit und Sicherheit darf vom Gesetzgeber neu justiert, die Gewichte dürfen jedoch von ihm nicht grundlegend verschoben werden." Kritisch zu letzterem: *V. Götz* § 41 Innere Sicherheit, in: H. Kube u.a. (Hrsg.) Leitgedanken des Rechts, FS Kirchhof, 2013, 457 (462 ff.). Zur Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse: *W. Brugger* und *C. Gusy* Gewährleistung von Freiheit und Sicherheit (o. Fn. 14), VVDStRL 63 (2004), 103 ff. und 151 ff.

gen zu warnen. Die immer wieder plakatierte Folie des totalitären NS-Staates und seiner GESTAPO etwa kann insoweit nur als eine angesichts der Realitäten und Institutionen des demokratischen Rechtsstaates zum Glück fern liegende Mahnung mit begrenzter Direktionskraft verstanden werden.[72] Hilfreicher erscheint der rechtsvergleichende Blick auf die staatliche Informationserfassung in anderen demokratischen Gemeinwesen. So wird etwa die internationale Auseinandersetzung um die Vorratsdatenspeicherung regelmäßig auf der Basis von Ausgestaltungen geführt, die deutlich weiter gehen, als der aktuelle Entwurf der Bundesregierung.[73] Dies kann Anlass bieten, die Frage der verfassungsrechtlichen Schranken dieser Form der Datenbevorratung und des Datenzugriffs auch hierzulande zurückhaltender zu beurteilen.[74]

---

[72] Ähnlich: *M. Kötter* (o. Fn. 11), Der Staat 43 (2004), 371 (393 ff.).

[73] Vgl. dazu das Urt. des English High Court v. 17.7.2015, in David Davis and Ors v The Secretary of State for the Home Department [2015] EWHC 2092 (Admin) Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014, in der das Gericht die britischen Bestimmungen zur Vorratsdatenspeicherung (nur) deshalb verwarf, weil diese einen Zugriff auch bei geringfügigen Straftaten vorsahen und nicht von der vorherigen Anordnung durch ein Gericht oder eine unabhängige Verwaltungsbehörde abhängig machten. Vgl. auch das Urteil des Österreichischen VfGH v. 27.6.2014, Az. G 47/2012-49 u.a., Rn. 166 ff., mit dem der Verfassungsgerichtshof die Regelung zur Vorratsdatenspeicherung in Österreich zwar *in concreto* verworfen, zugleich aber eine verfassungs- und EMRK-konforme Ausgestaltung für möglich erklärt hat; dazu: *M. Flora* The Unlawfulness of Data Retention confirmed by the Court of Justice of the European Union (CJEU) and the Austrian Constitutional Court (VfGH), EuCML 2015, 102 ff. Vgl. insoweit auch das Urteil der Rechtbank Den Haag v. 11.3.2015, Az. C/09/480009 / KG ZA 14/1575, mit dem dieses das niederländische Gesetz zur Vorratsspeicherung von TK-Verkehrs- und Standortdaten (Wet bewaarplicht telecommunicatiegegevens – Wbt) vorläufig außer Kraft gesetzt hat. Das Gericht hielt die Vorratsdatenspeicherung auch mit Blick auf die vom EuGH entwickelten Vorgaben für grundsätzlich mit dem grundrechtlichen Privatheitsanspruch vereinbar, rügte aber die fehlende Pflicht, die gespeicherten Daten innerhalb des Unionsgebiets zu speichern und eine hinreichend enge Fassung der Zugriffsbefugnisse. Näher zu der Entscheidung *S. Schweda* Niederlande: Vorratsdatenspeicherung einstweilig gestoppt, ZD-Aktuell 2015, 4624. In der US-amerikanischen Debatte wird eine wesentlich weitergehende Vorratsdatenspeicherung sogar als Instrument der Einhegung der informationellen Zugriffe der Sicherheitsbehörden verstanden, näher zum sog. USA-Freedom-Act v. 2.6.2015, https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048enr.pdf. Kritisch dazu: *E. Berman* The Two Faces of the Foreign Intelligence Surveillance Court (August 7, 2015) abrufbar unter: http://ssrn.com/abstract=2250123 oder http://dx.doi.org/10.2139/ssrn.2250123.

[74] IdS auch *F. Wollenschläger* Schriftliche Stellungnahme zur öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages am 21.9.2015, https://www.bundestag.de/blob/388296/e7137f2ea57c528846b018e69104cfd3/wollenschlaeger-data.pdf.

2. *Die Deprivilegierung der Geheimdienste*

Zugleich dürfen die im Zuge der NSA-BND-Affäre deutlich gewordenen Gefahren eines umfänglichen staatlichen Informationszugriffs nicht ignoriert werden. Im Vordergrund der nachfolgenden Reformüberlegungen steht deshalb die Tätigkeit der Geheimdienste.[75] Dafür spricht zum einen die besondere Dimension des geheimdienstlichen informationellen Zugriffs, der gegenüber selbst Vorhaben wie die Vorratsdatenspeicherung vergleichsweise geringfügig anmuten. Dafür spricht zum anderen der Umstand, dass es im geheimdienstlichen Bereich an Grenzziehungen noch weitgehend fehlt.[76] Aus sicherheitsrechtlicher Perspektive wird dies regelmäßig unter Hinweis auf die nicht vorhandenen operativen Möglichkeiten der Geheimdienste gerechtfertigt. Ihr Fehlen soll eine effektive Begrenzung der geheimdienstlichen informationellen Zugriffe zumindest weithin entbehrlich machen.[77]

In der Sache kann diese pauschale Privilegierung der Nachrichtendienste aber allenfalls sehr eingeschränkt überzeugen. Sie verkennt insbesondere den allgemeinen Charakter von Informationen. Diese können ganz unabhängig von eigentlich operativen Möglichkeiten eine Verwendung finden, die für Betroffene schwerste Konsequenzen zeitigen kann.[78] Hier droht eine

---

[75] Vgl. dazu aus übergreifender europäischer Perspektive auch das Thesenpapier 2/2015 des Menschenrechtskommissars des Europarates *N. Muižnieks* Demokratische und wirksame Aufsicht über die staatlichen Nachrichtendienste, v. 5.6.2015, https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2796364&SecMode=1&DocId=2301362&Usage=2.

[76] Zu den hier außer Betrachtung bleibenden besonderen Schwächen auch des Rechtsschutzes gegen die strategische Überwachung durch den BND: BVerwG, Urt. v. 28.5.2014 – 6 A 1/13, NVwZ 2014, 1666 ff.; ablehnend dazu: *P. Schantz* Rechtsschutz gegen die strategische Fernmeldeüberwachung: Ein „blinder Fleck" im Rechtsstaat?, NVwZ 2015, 873 ff.; *H. Goerlich* E-Mail-Überwachung von Anwälten durch den BND – und kein Rechtsschutz?, AnwBl 2014, 979 ff.

[77] *H. A. Wolff* (o. Fn. 1), DVBl 2015, 1076 (1078). Diese Logik lag – und liegt zum Teil bis heute – auch der eher großzügigen Rechtsprechung des Bundesverfassungsgerichts zugrunde, vgl. etwa BVerfGE 100, 313 (383, Rn. 240 ff.) – Strategische Telekommunikationsüberwachung BND (G 10 II); BVerfGE 133, 277 (325, Rn. 116 ff.) – Antiterrordatei. Dagegen betont BVerfGE 125, 260 (Rn. 233) – Vorratsdatenspeicherung, dass die fehlenden operativen Möglichkeiten der Geheimdienste zugleich „das Gewicht zur Rechtfertigung solcher Eingriffe" verringerten, weil „durch bloße Informationen der Regierung [...] Rechtsgutverletzungen nicht verhindert werden" könnten. Dies sei „erst möglich durch Folgemaßnahmen der für die Gefahrenabwehr zuständigen Behörden, deren verfassungsrechtliche Begrenzungen bei der Datenverwendung nicht durch weitergehende Verwendungsbefugnisse im Vorfeld unterlaufen werden" dürften.

[78] Eine überlegene Informationsmacht staatlicher Sicherheitsbehörden kann auch in Demokratien zum Zwecke politischer Erpressung und Manipulation genutzt werden. Das historische Beispiel der Praktiken des langjährigen FBI-Direktors *J. Edgar Hoover* mag

Einschüchterung der Funktionsträger des demokratischen Gemeinwesens, die dessen elementare Funktionsbedingungen auch jenseits des Einzelfalls erheblich zu beeinträchtigen vermag.[79]

Im Übrigen ist die fehlende operative Funktionsweise der Nachrichtendienste ihrerseits auch in der Sache angesichts eines erweiterten Aufgabenfeldes und der gerade in den letzten Jahren beständig erweiterten Zusammenarbeit von Nachrichtendiensten und sonstigen Sicherheitsbehörden in einem Erosionsprozess befangen.[80]

---

dies veranschaulichen; vgl. dazu *R. G. Powers* Secrecy and Power: The life of J. Edgar Hoover, 1987; *C. Gentry* J. Edgar Hoover: The man and his secrets, 1991; *R. Hack* Puppetmaster: The Secret Life of J. Edgar Hoover, 2007; *B. Medsger* The Burglary: The Discovery of J. Edgar Hoover's Secret FBI, 2014. Wesentliche Erkenntnisse zum Missbrauch geheimdienstlich gewonnener Erkenntnisse vermitteln auch die Berichte des Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities von 1975/1976 (sog. Church-Committee), näher dazu *R. A. Miller* (o. Fn. 57), 2014, 11 ff.; *ders.* US National Security, Intelligence and Democracy – From the Church Committee to the War on Terror, 2009. Zu der in den USA sog. "parallel construction", dem verdeckten Gebrauch verdeckt (und illegal) erlangter Daten im unlängst bekannt gewordenen Fall der geheimen Vorratsdatenspeicherung durch die US-amerikanische Drug Enforcement Agency: *P. Beuth* Die Vorratsdatenspeicherung der USA, Zeit-Online v. 8.4.2015, http://www.zeit.de/digital/datenschutz/2015-04/metadaten-geheime-vorratsdatenspeicherung-usa-dea.

[79] Zutreffend zur gemeinwohlbezogenen Komponente des Schutzes der informationellen Selbstbestimmung insoweit bereits BVerfGE 65, 1 (54, Rn. 154) – Volkszählung; ebenso: BVerfGE 115, 166 (192, Rn. 87) – Kommunikationsverbindungsdaten. Zur Sorge vor dem sich einstellenden Gefühl des Überwachtwerdens auch EuGH, verb. Rs. C-293, 594/12, 8.4.2014 – Digital Rights Ireland, Rn. 37. Zum sog. „chilling effect" bereits früh: US-Supreme Court, Wieman v. Updegraff, 344 U.S. 183 (1952).

[80] Diese Zusammenarbeit und der sie begleitende intensive Informationsaustausch werden sich mit der weiteren Ausgestaltung und Entfaltung immer neuer gemeinsamer Einrichtungen eher intensivieren denn abschwächen; vgl. dazu etwa: *N.-F. Weisser* Das Gemeinsame Terrorismusabwehrzentrum (GTAZ) – Rechtsprobleme, Rechtsform und Rechtsgrundlage, NVwZ 2014, 142 ff. Wie insbesondere die Schwächen der Zusammenarbeit im Bereich der Bekämpfung der rechtsextremen NSU gezeigt haben, besteht dafür auch ein kaum abweisbarer Bedarf. Zur entsprechenden Einschätzung eines insoweit ungenügenden Informationsaustauschs und den sich daraus ergebenden Forderungen: Abschlussbericht des NSU-Untersuchungsausschusses, BT Drs. 17/14600, 853 ff.; *K. P. Bruch/B. Jost/E. Müller/H. Vahldieck* Abschlussbericht der Bund-Länder-Kommission Rechtsextremismus v. 30.4.2013, 193 ff., Rn. 446 ff. Die deutsche Diskussion zeigt hier im kleineren Maßstab Parallelen zur US-amerikanischen Debatte um den ungenügenden Informationsaustausch zwischen den US-Sicherheitsbehörden im Vorfeld der Anschläge vom 11. September 2001, näher dazu *S. Büsching* Innere Sicherheit in der USA nach 9/11, ZFAS Sonderheft 2/2011, 80 (83 ff.). Zu gesetzgeberischen Konsequenzen aus der NSU-Affäre vor allem hinsichtlich einer besseren Koordination der Strafverfolgung: Gesetz zur Umsetzung von Empfehlungen des NSU-Untersuchungsausschusses des Deutschen Bundestages v. 12. 6.2015, BGBl. I v. 19.6.2015, 925.

Auch das Bundesverfassungsgericht hat deshalb die Notwendigkeit einer Einschränkung der Privilegierung der Nachrichtendienste[81] in einer bislang noch zu wenig beachteten Passage der Entscheidung zur Vorratsdatenspeicherung ausdrücklich betont.[82] Die verfassungsrechtlichen Anforderungen für die Verwendung der hier gespeicherten Daten sollen danach für alle Eingriffsermächtigungen mit präventiver Zielsetzung und damit auch für die Verwendung durch die Nachrichtendienste gelten.[83] Dass mit diesen Vorgaben eine Verwendung der vorsorglich gespeicherten Telekommunikationsverkehrsdaten von Seiten der Nachrichtendienste in vielen Fällen ausscheiden dürfte, begründe keinen verfassungsrechtlich hinnehmbaren Anlass, die sich aus dem Verhältnismäßigkeitsgrundsatz ergebenden Voraussetzungen abzumildern.[84]

Soweit das Bundesverfassungsgericht den prinzipiellen Gleichklang der Eingriffsanforderungen für alle staatlichen Behörden in der Vorratsdatenspeicherungsentscheidung[85] mit der besonderen Intensität des hier beurteilten informatorischen Zugriffs begründet hat, besteht aller Anlass, dies auch auf die Überwachung der Internetkommunikation durch die Nachrichtendienste zu übertragen. Anders als bei der Vorratsdatenspeicherung werden hier nämlich nicht allein Meta- oder Verkehrsdaten, sondern auch Kommunikationsinhalte großflächig erfasst und ausgewertet. Der staatliche Zugriff ist darüber hinaus ein auch in der Fläche unmittelbarer und nicht

---

[81] Den hier formulierten neueren verfassungsgerichtlichen Erkenntnissen ist auch deshalb ausdrücklich zuzustimmen, weil das Gericht selbst sie in seiner Antiterrordateientscheidung zugunsten eines letztlich untauglichen Versuchs der kategorialen Abgrenzung von Polizei und Nachrichtendiensten wieder verwischt hat, vgl. BVerfGE 133, 277 (325, Rn. 116 ff.) – Antiterrordatei; zu Recht kritisch hierzu: *M. Baldus* (o. Fn. 11) 1 (14).

[82] Ähnlich zuvor auch schon BVerfGE 120, 274 (328 ff., Rn. 246 ff.) – Online-Durchsuchung, wo das Gericht angesichts der potentiellen Schwere des grundrechtlichen Eingriffs durch Zugriff auf die privat genutzten informationstechnischen Systeme den grundsätzlichen Gleichklang der verfassungsrechtlich Anforderungen aus dem Verhältnismäßigkeitsgrundsatz für alle staatlichen Behörden betont und zugleich feststellt, dass insoweit u.U. auch der generelle Ausschluss des entsprechenden Instrumentariums für die Nachrichtendienste geboten sein kann: „Auch wenn es nicht gelingen sollte, speziell auf im Vorfeld tätige Behörden zugeschnittene gesetzliche Maßgaben für den Eingriffsanlass zu entwickeln, die dem Gewicht und der Intensität der Grundrechtsgefährdung in vergleichbarem Maße Rechnung tragen wie es der überkommene Gefahrenbegriff etwa im Polizeirecht leistet, wäre dies kein verfassungsrechtlich hinnehmbarer Anlass, die tatsächlichen Voraussetzungen für einen Eingriff der hier vorliegenden Art abzumildern."

[83] BVerfGE 125, 260 (331, Rn. 232) – Vorratsdatenspeicherung; unter Hinweis auf BVerfGE 120, 274 (329 f., Rn. 251 ff.) – Online-Durchsuchung.

[84] BVerfGE 125, 260 (332, Rn. 234) – Vorratsdatenspeicherung; unter Hinweis auf BVerfGE 120, 274 (331, Rn. 256 ff.) – Online-Durchsuchung.

[85] Ebenso auch in der vorangegangenen Entscheidung zur Online-Durchsuchung, vgl. die N. o. in Fn. 84.

lediglich ein anlass- und einzelfallbezogener. Die verfassungsgerichtlichen Anforderungen begründen deshalb für das Handeln der Nachrichtendienste einen substantiellen normativen Nachholbedarf, der gegenüber den eher punktuell erforderlichen weiteren verfassungsrechtlichen Korrekturen des informationellen Handelns der sonstigen Sicherheitsbehörden[86] vorrangig anzugehen ist.[87]

3. *Transparenz und Kontrolle*

Zu den strukturellen verfassungsrechtlichen Antworten auf die in jüngerer Zeit bekanntgewordenen staatlichen Informationszugriffe muss eine verstärkte Verpflichtung zur Transparenz[88] des Handelns auch der Geheimdienste gehören.[89] Die größtmögliche Transparenz staatlichen Handelns bei gleichzeitig größtmöglicher Rücksichtnahme auf die Privatheit des Einzelnen zeichnet den demokratischen Rechtsstaat aus und hebt ihn positiv von anderen Gesellschaftsordnungen ab.[90] Der staatliche informationelle Zugriff auf die bürgerliche Privatsphäre und ein geheimes Vorgehen der Staatsorgane sind hier nur ausnahmsweise gestattet und bedürfen stets einer verfassungsrechtlich tragfähigen Rechtfertigung. Der pauschale Hinweis auf die Natur der geheimdienstlichen Tätigkeit genügt dafür nicht.[91] Viel-

---

[86] Zu Neuordnungsvorstellungen im Kriminalpräventionsrecht auch jenseits verfassungsrechtlicher Vorgaben eingehend: *M. Bäcker* (o. Fn. 15), 2015, 379 ff.

[87] Dies auch deshalb, weil für die bislang anspruchsvolle deutsche Regulierung des informationellen Handelns der Sicherheitsbehörden angesichts der sich hier abzeichnenden europäischen Teilharmonisierung eher eine Relativierung denn eine Weiterentwicklung absehbar ist.

[88] Das Bundesverfassungsgericht hat Transparenzverpflichtungen auch und gerade hinsichtlich geheimer staatlicher Informationszugriffe formuliert und konturiert, vgl. dazu BVerfGE, 103, 142 (151 f., Rn. 27 ff.) – Wohnungsdurchsuchung; vgl. auch BVerfGE, 109, 279 (360 ff., Rn. 277 ff.) – Großer Lauschangriff; BVerfGE 125, 260 (Rn. 240 ff.) – Vorratsdatenspeicherung. Die hier entwickelten Vorgaben gelten aber in erster Linie der durch regelmäßig nachträgliche Unterrichtung zu gewährleistenden Transparenz gegenüber den Betroffenen; vgl. dazu auch Schweizerisches Bundesgericht, 1C 653/2012 vom 1.10.2014, EuGRZ 2014, 683 (690). Vor allem hinsichtlich der Tätigkeit des Bundesnachrichtendienstes läuft eine solche Verpflichtung aus sachlichen Gründen jedoch regelmäßig leer.

[89] Zur Bedeutung der Transparenz im hier interessierenden Kontext, *G Greenwald* No Place to Hide: Edward Snowden, the NSA and the Surveillance State, 2014: „Transparency is the only real antidote."

[90] *B. W. Wegener* Der geheime Staat, 2006, 387 ff., abrufbar unter http://www.oer2.jura.uni-erlangen.de/lehrstuhlinhaber/habil.pdf.

[91] Anders aber erneut der Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, BR-Dr 123/15 33, der eine „höhere Regelungsdichte" im Gesetz als „nicht nötig und auch untunlich" ablehnt, „da das Nähere nachrichtendienstlicher Methoden naturgemäß Geheimschutzanforderungen unterliege". Zustimmend:

mehr ist jeweils im Einzelfall zu prüfen, ob, inwieweit und gegenüber wem Geheimhaltung rechtfertigungsfähig ist. Der technisch induzierte Verlust an bürgerlicher Privatheit muss durch eine verfassungsrechtliche Einschränkung des geheimen staatlichen Handelns nach Möglichkeit kompensiert werden.

Die Geheimhaltung im Bereich der Nachrichtendienste muss deshalb unter verfassungsrechtlichen Vorzeichen durch eine deutlich intensivierte Kontrolle durch Öffentlichkeit und Parlament ergänzt und ganz allgemein zurückgeschnitten werden. Die NSA-BND-Affäre hat deutlich gemacht, dass wesentliche Strukturelemente des informationellen Zugriffs insbesondere des Bundesnachrichtendienstes weder den parlamentarischen[92] noch – jedenfalls soweit man bereit ist, den entsprechenden Bekundungen der Bundesregierung Glauben zu schenken – den exekutiven Aufsichtsorganen bekannt waren. Das hier erneut[93] offenbar gewordene Kontrollversagen[94] und das hierdurch ermöglichte geheime Eigenleben der Dienste widersprechen den Fundamentalbedingungen der viel beschworenen freiheitlich demokratischen Grundordnung.

Allgemeine, aggregierte Informationen über Art und Ausmaß der geheimdienstlichen Informationszugriffe müssen deshalb künftig weit mehr als bislang aus der Geheimhaltung herausgenommen und damit öffentlich diskutiert werden.[95] Die Geheimhaltungspflichten der Mitglieder der jewei-

---

J. Lampe (o. Fn. 19), NStZ 2015, 361 (364 ff.), der zwar zunächst feststellt, die Konstruktion einer durch geheime Dienstvorschrift konkretisierten Ermächtigung sei „wohl einzigartig", ihre „Einordnung in das rechtsstaatliche Normengefüge ‚bislang wenig diskutiert'" und „im demokratisch verfassten Rechtsstaat, der keine „Panzerschrankgesetze" kennt, an sich eine Unmöglichkeit"; die Konstruktion a.E. aber unter Heranziehung wenig klarer Maßstäbe doch für verfassungsrechtlich tragfähig erachtet und für die Tätigkeit des BND noch weitergehend als bislang nutzen will.

[92] Zu den insoweit fehlenden Kontrollrechten der G-10-Kommission und der ungenügenden Informationspraxis der Bundesregierung gegenüber dem Parlamentarischen Kontrollgremium bereits früh *B. Huber* (o. Fn. 44), NJW 2013, 2572 (2575).

[93] Vgl. dazu aus historischer Perspektive: *J. Foschepoth* Überwachtes Deutschland (o. Fn. 17), [4]2014. Schon 2009 sprach die Oppositionspartei Bündnis 90/DIE GRÜNEN im seinerzeitigen BND-Untersuchungsausschuss davon, Teile des BND seien außer Kontrolle geraten und hätten der US-Seite unbegrenzt und unkontrolliert Informationen über deutsche Terrorverdächtige gegeben, die für Verschleppungen und Verhöre unter Folter genutzt werden konnten und wurden, BT Drs. 16/13400, 889.

[94] Kritisch zu den Funktionsbedingungen der parlamentarischen Geheimdienstkontrolle: *J.-H. Dietrich* Reform der parlamentarischen Kontrolle der Nachrichtendienste als rechtsstaatliches Gebot und sicherheitspolitische Notwendigkeit, ZRP 2014, 205 ff. mwN.

[95] Vgl. dazu auch BVerfGE 113, 348 (376, Rn. 117) – Präventive Telekommunikationsüberwachung: „Für Ermächtigungen zu Überwachungsmaßnahmen verlangt das Bestimmtheitsgebot zwar nicht, dass die konkrete Maßnahme vorhersehbar ist, wohl aber, dass die betroffene Person grundsätzlich erkennen kann, bei welchen Anlässen und unter welchen

ligen parlamentarischen Kontrollgremien sind entsprechend zu beschränken.[96] Wie der Fall der mittlerweile eingestellten Ermittlungsmaßnahmen gegen „netzpolitik.org" veranschaulicht, darf es nicht der Exekutive selbst überlassen bleiben, Informationen über Art und Ausmaß der allgemeinen eigenen Überwachungspraxis als geheim einzustufen und damit der öffentlichen Auseinandersetzung zu entziehen.[97] Die einschlägige öffentliche Berichterstattung ist auch weiterhin verfassungsgerichtlich gegenüber exekutiven Zugriffen in Schutz zu nehmen.[98] Zu denken ist zudem an eine regelmäßige Berichtspflicht der Bundesregierung hinsichtlich der Tätigkeit der Geheimdienste, wie sie das Grundgesetz in ähnlichem Zusammenhang an anderer Stelle bereits vorsieht.[99]

Neben einer substantiellen personellen Stärkung der parlamentarischen Kontrollgremien[100] ist auch die Schaffung des Amts eines vom Parlament

---

Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist." Zu den US-amerikanischen gerichtlichen Auseinandersetzungen zwischen dem Telekommunikationsanbieter Merrill und dem FBI über die Verpflichtung zur Verschwiegenheit hinsichtlich der sicherheitsbehördlichen Zugriffe: *N. Schnarrenberger* Merrill vs. FBI: National Security Letter-Knebel erstmalig komplett aufgehoben, 18.9.2015, https://netzpolitik.org/2015/merrill-vs-fbi-national-security-letter-knebel-erstmalig-komplett-aufgehoben/. Jedenfalls im Ansatz zu restriktiv deshalb BVerwG, Beschl v. 20.7.2015, 6 VR 1.15 zum generell fehlenden Auskunftsanspruch der Presse hinsichtlich der Tätigkeit des BND.

[96] Dafür auch *D. Deiseroth* (o. Fn. 18), ZRP 2013, 194 (196 f.) m. weitergehenden Detailvorschlägen.

[97] Als Negativbeispiel für eine entsprechend weitgehende Geheimhaltung kann etwa die Antwort der Bundesregierung auf eine Kleine Anfrage in BT Drs. 17/9640 gelten, in der die Bundesregierung bspw. auch die Antwort auf die allgemeine Frage nach der Überwachung des Frankfurter Internet-Netzknotens DE-CIX für „Geheim" erklärte und damit der öffentlichen Diskussion zu entziehen suchte.

[98] Vgl. BVerfGE 20, 162 (178 ff.); 77, 65 (74 ff.); 117, 244 (258 ff.); BVerfG, Beschl. v. 10.12.2010 – 1 BvR 1739/04 –, NJW 2011, 1859 (1860); BVerfG, Beschl. v. 13.7.2015, 1 BvR 1089–1090, 2480/13. Zu einer möglichen Änderung des Straftatbestandes des Landesverrats, die die bloße journalistische Publikation von Informationen aus dem Begriff der Beihilfe ausklammerte: Bundesjustizminister *H. Maas* Presse und Zivilgesellschaft – Wer braucht wen?, Zeitungskongress 2015 des BDZV, http://www.bmjv.de/SharedDocs/Reden/DE/2015/20150921_BDZV.html?nn=1477162. Zu Überlegungen zu einem auch internationalrechtlich zu stärkenden „Whistleblower"-Schutz: *D. Deiseroth* (o. Fn. 18), ZRP 2013, 194 (196 f.); *C. Bäcker* Whistleblower im Amt – Zwischen Verschwiegenheitspflicht und Verfassungstreue, Die Verwaltung 2015, (i.E.).

[99] Vgl. Art. 13 Abs. 6 GG hinsichtlich des polizeilichen informationellen Zugriffs auf Wohnungen.

[100] Die Forderung nach einer substantiellen personellen und technologischen Stärkung der parlamentarischen Kontrolle insbesondere durch das Parlamentarische Kontrollgremium und die G 10-Kommission ist in der aktuellen Diskussion weit verbreitet, vgl. dazu bereits Bericht des Parlamentarischen Kontrollgremiums über die Kontrolltätigkeit gemäß § 13 PKGrG, BT Drs. 18/217, 19.12.2013, 14; Eckpunktepapier der SPD-Bundestagsfraktion, (o. Fn. 28), 14. Allen Bedenken hinsichtlich zu kleinteiliger Vorgaben zum Trotz kann auch

zu bestellenden Bundesbeauftragten für die Geheimdienste zu erwägen.[101] Dabei wird in der Sache vor allem darauf zu achten sein, dass die derzeit noch bestehenden kontrollfreien Tätigkeitsfelder – insbesondere der vom BND sog. „Routineverkehr" – einer effektiven parlamentarischen Kontrolle unterstellt werden.[102] Dafür muss vorgesehen werden, dass die parlamentarischen Kontrollgremien nicht allein auf der Grundlage jeweils spezifisch zugeschnittener gesetzlicher Verpflichtungen informiert werden, sondern ein grundsätzlich freies Informationsbeschaffungsrecht eingeräumt bekommen.[103] Die entsprechenden Informationsrechte sind um ihrer Funktionsfähigkeit willen grundsätzlich als Minderheitenrechte auszugestalten.[104]

Anlässlich der Auseinandersetzungen um die parlamentarische Kontrolle des Bundesnachrichtendienstes und konkret um die Einsicht in die notorische NSA-BND-Selektorenliste[105] wird das Bundesverfassungsge-

---

diese Forderung als verfassungsrechtliche begriffen werden. Das Bundesverfassungsgericht hat schon in seiner Entscheidung zur Telekommunikationsüberwachung von 1999 festgestellt, dass dafür Sorge zu tragen sei, dass die G 10-Kommission angesichts der seinerzeit erheblich ausgeweiteten Überwachungstätigkeit personell so ausgestattet sei, dass sie ihrer Kontrollaufgabe in effektiver Weise nachzukommen vermöge: vgl. BVerfGE 100, 313 (Rn. 306) – Strategische Telekommunikationsüberwachung BND (G 10 II), (gleiches soll danach auch für die Kontrolle der Landesbehörden gelten, soweit diesen unter Aufhebung des Fernmeldegeheimnisses erlangte Daten übermittelt werden). Vergleicht man den seinerzeit beurteilten Überwachungsumfang mit der aktuellen Überwachungssituation dürften verfassungsrechtlich substantielle Verbesserungen der parlamentarischen Kontrolle notwendig sein. Es erscheint auch verfassungsrechtlich fraglich, ob die entsprechende Kontrolltätigkeit wie bislang mit äußerst begrenztem personellen Einsatz und weithin ehrenamtlich geleistet werden kann.

[101] *J.-H. Dietrich* (o. Fn. 94), ZRP 2014, 205 (208) mwN. Dagegen aber: Eckpunktepapier der SPD-Bundestagsfraktion, (o. Fn. 28), 14.

[102] Für eine gesetzliche Verpflichtung des Bundeskanzleramts zur Bekanntgabe des BND-Auftragsprofils gegenüber der G 10-Kommission: Eckpunktepapier der SPD-Bundestagsfraktion, (o. Fn. 28), 10.

[103] Dafür auch: *J.-H. Dietrich* (o. Fn. 94), ZRP 2014, 205 ff. Vgl. dazu auch die Aussage des Vorstands des Betreibers des DE-CIX Internetknotens *K. Landefeld* v. 25.3.2015 in der Anhörung des NSA-Untersuchungsausschusses des Bundestages, wonach die Betreibergesellschaft bereits 2008 wegen des nach ihrer Ansicht rechtswidrigen Zugriffs des BND auf die Internetkommunikation Kontakt mit der G 10-Kommission habe aufnehmen wollen, daran aber durch das Kanzleramt gehindert worden sei, http://www.zeit.de/digital/datenschutz/2015-04/de-cix-bundesverwaltungsgericht-klage-bnd-ueberwachung.

[104] Zu den aus diesem Gedanken resultierenden Schwächen des sog. „Vorsitzendenverfahrens", vgl. BVerfGE 124, 78 (139, Rn. 166) – BND-Untersuchungsausschuss.

[105] Zu Recht kritisch zum verfassungsrechtlich untauglichen Versuch, das Untersuchungsrecht des NSA-Ausschusses durch einen von der Regierung bestellten Sonderermittler zu ersetzen: *E. Peters* Der Sonderermittler zum NSA-Untersuchungsausschuss – eine Mogelpackung?, VerfBlog, 2015/7/21, http://www.verfassungsblog.de/der-sonderermittler-zum-nsa-untersuchungsausschuss-eine-mogelpackung/.

richt Gelegenheit erhalten, die notwendige Transparenz des geheimdienstlichen Handelns im Verhältnis zur parlamentarischen Kontrolle neu zu definieren.[106] Es sollte sich dabei nicht von pauschalen Hinweisen auf vorgebliche außen- und sicherheitspolitische Notwendigkeiten beeindrucken lassen, hinter denen kaum mehr steht als der durchsichtige Versuch, sich der politischen Verantwortung zu entziehen.[107]

Bei dieser und nachfolgenden Entscheidungen zur Kontrolle der sachlichen Legitimation des exekutiven Geheimhaltungsverlangens muss das Bundesverfassungsgericht – wie es dies in seiner Rechtsprechung zu § 99 VwGO schon vor Jahren ganz allgemein als verfassungsrechtlich zwingend bezeichnet hat[108] – die einschlägigen Dokumente gegebenenfalls selbst kritisch durch eine eigene „in-camera"-Betrachtung prüfen.[109] Nur eine solche Praxis kann hinsichtlich des parlamentarischen wie des öffentlichen Informationsverlangens dem verfassungsrechtlichen Gebot effektiven Rechtsschutzes gerecht werden.[110]

---

[106] Klageschrift von *W. Ewer* v. 16.9.2015 zu finden bei *A. Biselli* Grüne und Linke verklagen Bundesregierung wegen vorenthaltener Selektorenliste, 17.9.2015, https://netzpolitik.org/2015/gruene-und-linke-verklagen-bundesregierung-wegen-vorenthaltener-selektorenliste/. Näher zu dem für die Abwägung von parlamentarischer Kontrolle und exekutivem Geheimhaltungsverlangen zentralen Topos: *P. Cancik* Der „Kernbereich exekutiver Eigenverantwortung" – zur Relativität eines suggestiven Topos, ZParl 2014, 885 ff.

[107] Treffend dazu bereits BVerfGE 124, 78 (134, Rn. 154) – BND-Untersuchungsausschuss: „In dem bloßen Umstand, dass das Bekanntwerden derartiger Informationen der Bundesregierung selbst im Hinblick auf ihren eigenen Umgang mit den betreffenden Erkenntnissen Unannehmlichkeiten bereiten könnte, läge keine Gefährdung des Staatswohls, sondern eine hinzunehmende verfassungsgewollte Folge der Ausübung des parlamentarischen Untersuchungsrechts."

[108] BVerfGE, 101, 106 (128, Rn. 90) – in-camera-Verfahren. Siehe auch: *W.-R. Schenke* in: Kopp/Schenke (Hrsg.), VwGO, 2015, § 99, Rn. 1 ff.; *H. Posser* in: Posser/Wolff (Hrsg.) VwGO, 2014, § 99, Rn. 1 ff.; *H. Lang* in: Sodan/Ziekow (Hrsg.) VwGO, 2014, § 99, Rn. 2 ff.; *R. Rudisile* in: Schoch/Schneider/Bier (Hrsg.) VwGO, 2015, § 99, Rn. 2a ff.; *A. Beutling* Neue Wege im Verwaltungsprozess – das „in camera"-Verfahren, DVBl 2001, 1252 ff.; *J. Margedant* Das „in camera"-Verfahren, NVwZ 2001, 795 ff.; *C. Bickenbach* Das „in camera"-Verfahren, BayVBl 2003, 295 ff.

[109] Eine entsprechende (Selbst-)Verpflichtung ist im Übrigen in der Rechtsprechung des EuGH allgemein anerkannt; vgl. dazu EuGH, C-300/11, 4.6.2013, Rn. 54 ff. (ZZ); verb. Rs. C-584, 593, 595/10 P, 18.7.2013, Rn. 126 ff. (Kadi II). Nach der Abgrenzung der Zuständigkeiten nach § 36 PUAG in seiner Auslegung durch das BVerfG (dazu etwa: BVerfG, 2 BvE 3/14, 4.12.2014, Rn. 37 – Zeugenvernehmung Edward Snowden) dürfte eine Zuständigkeit des Bundesgerichtshofs für entsprechende Streitentscheidungen ausscheiden. Im Übrigen würde sich auch für ihn eine Verpflichtung zur „in-camera"-Entscheidung ergeben.

[110] Wie das Verfahren zur Aktenvorlage im Rahmen des BND-Untersuchungsausschuss gezeigt hat, ist die Effektivität entsprechender gerichtlicher Streitverfahren ohnehin prekär. Die Entscheidung des BVerfG, die den Antragstellern im Wesentlichen Recht gab und die restriktive Informationspraxis der Bundesregierung als verfassungswidrig verwarf

4. *Verrechtlichung geheimdienstlichen Handelns*

Die Tätigkeit der Geheimdienste bedarf weiter einer nachholenden Verrechtlichung durch Ermächtigungsnormen, die die tatbestandlichen Voraussetzungen und Grenzen des nachrichtendienstlichen Handelns – in der Sprache des Bundesverfassungsgerichts – „normenklar" bestimmen. Die hiergegen naheliegenden Einwände, dies widerspreche dem Charakter der nachrichtendienstlichen Tätigkeit und bringe außerdem Probleme mit sich, die schon hinsichtlich der sonstigen informationsbezogenen Tätigkeit der Sicherheitsbehörden mit dem Begriff der „Verrechtlichungsfalle"[111] umschrieben werden, verfangen im Ergebnis nicht.[112] Eine rechtliche Blankoermächtigung zu beliebigem grundrechtsrelevantem Handeln kann unter dem Grundgesetz keine Anerkennung finden.[113]

Dies gilt auch für die Auffassung der Bundesregierung und des Bundesnachrichtendienstes, wonach dessen gegen Ausländer gerichtete Informationszugriffe keinen grundrechtlichen und weitergehend auch keinen sonstigen rechtlichen Einschränkungen unterliegen, sondern vielmehr allein auf der Basis der inhaltlich sehr unbestimmten allgemeinen gesetzlichen Aufgabenbeschreibung zulässig sein sollen. Entsprechende Informationen sollen demnach schrankenlos erhoben, ausgewertet, gespeichert und an ausländische Partnergeheimdienste übermittelt werden können. Diese in Fachkreisen eher spöttisch als „Weltraumtheorie"[114] bekannt gewordene These ist mit Art. 10 GG nicht vereinbar.[115] Sie ist aber nach wie vor

---

(BVerfGE 124, 78 – BND-Untersuchungsausschuss), erfolgte erst nach Abschluss der Arbeiten des Untersuchungsausschusses. Weil und soweit sie – ohne „in-camera"-Einsicht in die betroffenen Unterlagen – lediglich eine unzureichende Begründung der Geheimhaltung feststellte, erlaubte sie zumindest theoretisch eine nachholende Begründung der Geheimhaltung und damit eine weitere zeitliche Verzögerung der Informationsbegehren.

[111] Allg. zum Begriff: *E. Gurlit* Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035 (1041); *H.-P. Bull* Zweifelsfragen an die informationelle Selbstbestimmung – Datenschutz als Datenaskese, NJW 2006, 1617 (1617).

[112] Anders als im Bereich des allgemeinen Datenschutzes droht hier schon der Sache nach insbesondere nicht die Gefahr einer „Verrechtlichung des Alltäglichen"; zu dem Begriff *M. Thiel* „Entgrenzung" der Gefahrenabwehr, 2011, 264 f.

[113] Dies gilt auch in Fällen großer Gefahren: BVerfGE 100, 313 (383, Rn. 221, 242) – Strategische Telekommunikationsüberwachung BND (G 10 II).

[114] Vgl. Eckpunktepapier der SPD-Bundestagsfraktion, (o. Fn. 28), 15; *K. Biermann* Die Anarchos vom BND, zeit-online v. 14.11.2014, http://www.zeit.de/politik/deutschland/2014-11/bnd-bundesnachrichtendienst-gesetz-grundrecht. Frühere Bezeichnung: „offener Himmel"; ablehnend dazu bereits: *B. Huber* (o. Fn. 44), NJW 2013, 2572 (2575 f.).

[115] *B. Huber* (o. Fn. 44), NJW 2013, 2572 (2575 f.); ebenso auch *M. Bäcker* Stellungnahme NSA-Untersuchungsausschuss, 2014, 18 ff.; *W. Hoffmann-Riem* Stellungnahme NSA-Untersuchungsausschuss, 2014, 11 f.; *H.-J. Papier* Stellungnahme NSA-Untersuchungsausschuss, 2014, 7; die Stellungnahmen aller Sachverständigen sind abrufbar unter:

Grundlage der alltäglichen Praxis. Anders als dies die Bundesregierung und der BND zumindest implizit unterstellen, handelt es sich bei Art. 10 GG erkennbar nicht um ein Deutschengrundrecht.[116] Auch fehlt es – wie das Bundesverfassungsgericht bereits festgestellt hat – hinsichtlich des Handelns deutscher Behörden nicht an einem den Anwendungsbereich der Grundrechte eröffnenden unmittelbaren Bezug zu einer deutschen hoheitlichen Tätigkeit.[117]

5. *Grenzen der Informationserhebung und -verwendung*

Eine verfassungsrechtlich hinreichend bestimmte Grenzziehung fehlt der Informationserhebung und Informationsverwendung durch die Nachrichtendienste darüber hinaus ganz allgemein. Die im sonstigen Sicherheitsrecht teils freiwillig gesetzgeberisch gezogenen, teils verfassungsgerichtlich erzwungenen Grenzen lassen sich hier allenfalls in Ansätzen ausmachen. Sie setzen der Informationsgewinnung durch die Geheimdienste keine wirksamen Grenzen. Zur Veranschaulichung müssen hier Beispiele genügen.[118] So hat der Gesetzgeber etwa die sog. „strategische

---

https://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848; *F. Becker* (o. Fn. 1), NVwZ 2015, 1335 (1339). A.A. für eine Informationserhebung im Ausland über das Ausland: *C. Gusy* in: Schenke/Graulich/Ruthig Sicherheitsrecht des Bundes, 2014, BNDG § 1, Rn. 51 ff.

[116] Ablehnend zu der in vielem parallelen Auffassung der US-Regierung, sie sei bei exterritorialen Tätigkeiten (oder bei solchen, die sich auf exterritoriale Kommunikationsvorgänge bezögen) nicht an die von ihr eingegangenen menschenrechtlichen Verpflichtungen gebunden: *D. Korff* (o. Fn. 60), 2014, 30 ff.

[117] Problematisch erscheinen deshalb nach geltender Verfassungslage auch die viel aber höchst ungenau diskutierten Abstufungen des hier zu gewährleistenden grundrechtlichen Schutzniveaus gegenüber Ausländern. Die entsprechenden Schwierigkeiten werden augenscheinlich, wenn insoweit eine Art grundrechtliche Binnenabstufung gegenüber Deutschen, EU-Ausländern, Staatsangehörigen verbündeter Staaten und sonstigen Ausländern diskutiert wird, vgl. insoweit Eckpunktepapier SPD-Bundestagsfraktion, (o. Fn. 28), 11. Mit der geltenden Verfassungslage scheinen diese Differenzierungen kaum vereinbar. Der zur Rechtfertigung eines eingeschränkten grundrechtlichen Schutzes angeführte Umstand, die betroffenen Ausländer unterlägen jenseits der Kommunikationsüberwachung regelmäßig nicht dem unmittelbaren operativen Zugriff deutscher Behörden, verfängt jedenfalls dann nur begrenzt, wenn – wie dies der Praxis der Nachrichtendienste entspricht – die Kommunikationsdaten auch großflächig mit Nachrichtendiensten anderer Staaten geteilt werden, denen ein solcher unmittelbarer Zugriff möglich ist. Vgl. dazu die Aussage des vormaligen NSA-Direktors *M. Hayden:* „We kill people based on Metadata", https://www.youtube.com/watch?v=UdQiz0Vavmc. Zur Problematik auch Eckpunktepapier SPD-Bundestagsfraktion, (o. Fn. 28), 15.

[118] Zu weiteren Zweifeln an der Verfassungskonformität der Ermächtigungen zum Einsatz von Mitteln zur heimlichen Informationsbeschaffung nach § 3 BNDG und § 8 BVerfSchG bereits o. Fn. 91 und *C. Gusy* in: Schenke/Graulich/Ruthig Sicherheitsrecht des Bun-

Telekommunikationsüberwachung" gegenüber dem vom Bundesverfassungsgericht 1999 beurteilten Sachverhalt allein dadurch beträchtlich ausgeweitet, dass er sie auf den zuvor ausgeklammerten Bereich[119] der leitungsgebundenen Kommunikation und damit auf die gesamte Internetkommunikation erstreckt hat. Zur Kompensation hat er in § 10 Abs. 4 S. 3 G 10 den Anteil der auf den leitungsgebundenen Übertragungswegen zu überwachenden Informationen auf höchstens 20% der jeweils zur Verfügung stehenden Übertragungskapazität beschränkt. In der Praxis ergeben sich aus dieser Bestimmung aber keine greifbaren Einschränkungen der Tätigkeit des Bundesnachrichtendienstes.[120] Bundesregierung und BND gehen vielmehr offenbar davon aus, dass auch eine vollständige Spiegelung[121] des auf dem jeweiligen Übertragungsweg anfallenden Datenstroms zulässig ist.[122]

Typisch für die fehlende Begrenzungsfunktion des geltenden Rechts sind auch die Regelungen zur Abgrenzung der strategischen von der einzelfallbezogenen Kommunikationsüberwachung. So verbietet § 5 Abs. 2 S. 2 Nr. 1 G 10 die Verwendung von Suchbegriffen die Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen. Nach Auffassung des Bundesverfassungsgerichts

---

des, 2014, BNDG § 3, Rn. 4. Ablehnend zur Frage, inwieweit die entsprechenden Bestimmungen überhaupt als Ermächtigungsnormen verstanden werden können: OLG Düsseldorf, Urt. v. 6.9.2013, 5 StS 5/10, NStZ 2013, 590; näher dazu *J. Lampe* (o. Fn. 19), NStZ 2015, 361 ff. mwN. Vgl. auch die beabsichtigte Neuregelung durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, BR Drs. 123/15 und BR Drs. 382/15.

[119] Vgl. dazu BVerfGE 100, 313 (376 f., Rn. 220 ff.) – Strategische Telekommunikationsüberwachung BND (G 10 II).

[120] Skeptisch dazu auch Eckpunktepapier der SPD-Bundestagsfraktion, (o. Fn. 28), 11.

[121] Vgl. die entsprechende Darstellung der Bundesregierung in BT Drs. 17/9640, 4 „vollständige Kopie der Telekommunikationen [...], die in den angeordneten Übertragungswegen vermittelt wird"; ebenso auch die Feststellung des BVerwG, Urt. v. 28.5.2014 – 6 A 1/13, NVwZ 2014, 1666 (1668, Rn. 24).

[122] Zum einen sei die gesetzliche Beschränkung auf die maximale Übertragungskapazität bezogen, die aber von den Telekommunikationsanbietern ihrerseits aus technischen Gründen im Schnitt kaum dauerhaft über 20% genutzt werde. Die gesetzlich bestimmte Beschränkung betreffe zum anderen erst die mittels inhaltlicher oder formaler Selektoren erfolgende Auswertung dieses Datenstroms, die unter diesen Rahmenbedingungen stets weniger als 20% der potentiellen Kapazität erfasse. Im Ergebnis muss man nach unwidersprochenen Medienberichten davon ausgehen, dass die entsprechende Informationserfassungspraxis des BND aktuell eher durch technische und finanzielle denn durch rechtliche Grenzen beschränkt wird. So soll der BND täglich allein etwa 220 Millionen Metadatensätze erfassen und speichern, von denen ihrerseits bis zu 1,3 Milliarden Daten pro Monat an die NSA weitergeleitet werden, vgl. *K. Biermann*, BND liefert NSA 1,3 Milliarden Metadaten – jeden Monat, 12.5.2015, http://www.zeit.de/politik/deutschland/2015-05/bnd-nsa-milliarden-metadaten.

ist die entsprechende Beschränkung verfassungsrechtlich zwingend, weil „ohne ein solches Verbot [...] die Verhältnismäßigkeit angesichts der Verdachtslosigkeit der Eingriffe, der Breite der erfassten Fernmeldekontakte und der Identifizierbarkeit der Beteiligten nicht gewahrt" wäre.[123] Schon normativ gilt die Beschränkung aber zum einen regelmäßig nicht für Telekommunikationsanschlüsse im Ausland, ohne dass dafür eine hinreichende verfassungsrechtliche Rechtfertigung erkennbar wäre.[124] Zum anderen verfehlt die Norm auch insoweit ihr Ziel, als sie sich allein auf Telekommunikations*anschlüsse* bezieht. Im Bereich der Internetkommunikation ist eine Identifizierung einzelner Teilnehmer regelmäßig auch ohne einen Bezug zu konkreten Anschlüssen – etwa über ihre E-Mail-Adresse – möglich.[125]

Jedenfalls in der Praxis kennen die deutschen Nachrichtendienste schließlich offensichtlich keine wirksamen Beschränkungen hinsichtlich der Weitergabe der durch die eigene großflächige Kommunikationsüberwachung gewonnenen Daten an Partnergeheimdienste.[126] Die in diesem Zusammenhang in Berichten immer wieder angeführten relativ kleinen Zahlen übermittelter Einzelerkenntnisse[127] dürfen die Tatsache nicht verschleiern, dass insbesondere der BND massenhaft Rohdaten oder Daten erster Aufarbeitungsstufen etwa an die NSA weitergibt.[128] Während in der Literatur weithin die Auffassung vorherrscht, der Übermittlung stünden rechtlich anspruchsvolle Hürden entgegen,[129] scheint dies in der Praxis

---

[123] BVerfGE 100, 313 (384, Rn. 243) – Strategische Telekommunikationsüberwachung BND (G 10 II).

[124] Ebenso *B. Huber* (o. Fn. 44), NJW 2013, 2572 (2574); *F. Becker* (o. Fn. 1), NVwZ 2015, 1335 (1339).

[125] Zu den weiteren Einzelheiten eingehend *M. Bäcker* (o. Fn. 115), 14.

[126] Vgl. die Hinweise o. in Fn. 122. Diese Praxis steht in einem immerhin bemerkenswerten Kontrast zu den verfassungsgerichtlich bereits vergleichsweise eng konturierten Anforderungen an die Weitergabe von Informationen an deutsche Sicherheitsbehörden. Ein Austausch von Informationen zwischen Polizeibehörden und Nachrichtendiensten soll danach gesteigerten verfassungsrechtlichen Anforderungen unterliegen und nur ausnahmsweise zulässig sein. Näher zu dem insoweit geltenden informationellen Trennungsprinzip: BVerfGE 133, 277 – Antiterrordatei. Nach den Erkenntnissen des Bundesverfassungsgerichts folgt es nicht aus dem verfassungsrechtlich ungesicherten allgemeinen Trennungsgebot, sondern aus dem Grundrecht auf informationelle Selbstbestimmung. Kritisch zur Debatte um das Trennungsgebot: *M. L. Fremuth* Wächst zusammen, was zusammen gehört? – Das Trennungsgebot zwischen Polizeibehörden und Nachrichtendiensten im Lichte der Reform der deutschen Sicherheitsarchitektur, AöR 2014, 32 (46 ff.) mwN.

[127] Vgl. BT-Dr 17/8639, 7; 17/12773, 8; BT Drs. 18/218, 9.

[128] Vgl. bereits: *B. Huber* (o. Fn. 44), NJW 2013, 2572 (2576): „Über das wahre Ausmaß des Datenaustauschs lassen sich jedoch aus den Angaben zur Praxis nach § 7a G 10 keine Schlüsse ziehen."

[129] *W. Hoffmann-Riem* (o. Fn. 115), 12 f.; *M. Bäcker* (o. Fn. 115), 15, vgl. dort auch die Kritik an der gegenläufigen Praxis.

grundlegend anders gesehen und gehandhabt zu werden. In der Tat sind die entsprechenden Übermittlungsbestimmungen[130] mit Begriffen wie der „Wahrung außen- oder sicherheitspolitischer Belange der Bundesrepublik Deutschland" oder „erheblicher Sicherheitsinteressen ausländischer Staaten" denn auch nur äußerst vage und interpretationsoffen bestimmt. Für die erfasste ausländische Kommunikation sollen nach der oben geschilderten verfassungswidrigen Rechtsauffassung der Dienste und der Bundesregierung diese Beschränkungen ohnehin nicht greifen.

6. *Technologische Antworten und ihre rechtlichen Grenzen*

Die angesichts all dessen erforderlichen – hier nur grob umrissenen – neuen verfassungsrechtlichen Grenzziehungen des staatlichen Informationszugriffs werden durch zukünftige Technikentwicklungen – anders als dies viele je nach Standpunkt erhoffen oder befürchten – kaum entbehrlich werden. Zwar lassen sich schon heute erhebliche Anstrengungen beobachten, die elektronische Kommunikation mit Mitteln der Verschlüsselung gegen Zugriffe staatlicher oder privater Provenienz abzuschirmen. Die staatlichen Sicherheitsbehörden stehen solchen Bestrebungen – jedenfalls soweit sie eine effektive Abschirmung der Kommunikation auch gegen die von ihnen intendierten Zugriffe bedeuten könnten – aber ablehnend gegenüber.[131] Eben deshalb hat die NSA – erlauben Sie mir den lokalpatriotischen Hinweis – die elektronische Kommunikation – einschließlich der Telefonate – eines Erlanger Studenten mitgeschnitten, der als Mitentwickler an der Verschlüsselungstechnik Tor[132] arbeitete. Insbesondere die NSA[133] hat sich immer bemüht, die Entwicklung ihr gegenüber sicherer elektronischer Kommunikation nach Möglichkeit zu verhindern. Der Sache nach handelt es sich vordergründig allein um eine Art technologischen Wettlauf, zwischen intelligenter und alltagstauglicher Verschlüsselung einerseits und sicherheitsbehördlichen Aufklärungsbestrebungen andererseits. Verfassungsrechtlich stellt sich aber die Frage, inwieweit es dem Staat erlaubt, geboten oder verboten ist, die Entwicklung und Anwendung auch ihm gegenüber sicherer Verschlüsselung zu untersagen und zu bekämp-

---

[130] Vgl. insbesondere § 7a G 10.

[131] Zu Bestrebungen der indischen Regierung, die Möglichkeiten der Verschlüsselung gegenüber Sicherheitsbehörden legislativ zu beschränken: *T. Rudl* Recht auf Verschlüsselung: Indien zieht umstrittenen Gesetzentwurf zurück, 22.9.2015, https://netzpolitik.org/2015/recht-auf-verschluesselung-indien-zieht-umstrittenen-gesetzentwurf-zurueck/.

[132] Überblick zum Tor Netzwerk bei *M. Thiesen* Wie hoch ist der Preis der Anonymität? – Haftungsrisiken beim Betrieb eines TOR-Servers, MMR 2014, 803 ff.

[133] In Deutschland bemüht sich der BND um entsprechende Entschlüsselungsfähigkeiten, vgl. dazu das o. Fn. 22 BND-Strategiepapier.

fen.[134] In der IT-nahen journalistischen Szene werden schon entsprechende staatliche Absichtserklärungen als totalitär wahrgenommen.[135]

Demgegenüber ist auf die verfassungsrechtliche Zulässigkeit entsprechender Einschränkungen zu verweisen.[136] Das Bundesverfassungsgericht betont in seiner Rechtsprechung zu den verfassungsrechtlichen Grenzen staatlicher Informationszugriffe immer wieder die besondere Bedeutung der staatlichen Verantwortung für Sicherheit und Strafverfolgung.[137] Wie bereits skizziert anerkennt das Gericht dabei zu Recht keine absoluten

---

[134] Laut Medienberichten befindet sich etwa die US-Regierung derzeit bereits in entsprechenden rechtlichen Auseinandersetzungen mit Apple und anderen Kommunikations- bzw. Geräteanbietern. So soll Apple eine gerichtliche Anordnung zur Herausgabe von Kommunikationsdaten in einem Fall möglichen Waffen- und Drogenhandels mit dem Hinweis auf die Verschlüsselungstechnik seiner neuen Gerätegeneration als unmöglich verweigert haben, vgl. *M. Apuzzo/D. E. Sanger/M. S. Schmidt* Apple and Other Tech Companies Tangle With U.S. Over Data Access, New York Times v. 7.9.2015, http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=0.

[135] Vgl. *S. Lobo* SPIEGEL-Online v. 15.7.2015: „Der gefährlichste Mann Europas, David Cameron, steht kurz davor, faktisch WhatsApp und iMessage zu verbieten sowie insgesamt Privatnachrichten, die die Bezeichnung ‚privat' auch verdienen. Das dazugehörige Zitat des britischen Premierministers lautet: ‚Wollen wir in unserem Land Kommunikationsmittel zwischen Menschen erlauben, die wir [als Staat] nicht lesen können? Meine Antwort auf diese Frage ist: Nein, wir dürfen das auf keinen Fall erlauben.' Das ist ein Zitat, das Stalin nicht totalitärer hätte formulieren können. Ich empfinde diese Aussage als Katastrophe, als Aufkündigung ungefähr jeden Wertes, den ich mit einem demokratischen Europa verbinde. Zu den sicherheitspolitischen Notwendigkeiten einer effektiven Verschlüsselung auch: *S. Lobo* SPIEGEL-Online v. 28.1.2015, http://www.spiegel.de/netzwelt/web/sascha-lobo-warum-verschluesselung-unverzichtbar-ist-a-1015398.html. Am 4.11.2015 hat die britische Regierung die sog. „Draft Investigatory Powers Bill" vorgestellt, die Serviceprovider u.a. zur Mitarbeit bei der Zugänglichmachung auch verschlüsselter Kommunikation verpflichten soll, vgl. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf, Rn. 61 ff.

[136] Ähnliches dürfte für Einschränkungen hinsichtlich einer möglichen Auslagerung der sicherheitsrelevanten Daten in Drittländer gelten. Auch insoweit steht das Verfassungsrecht der Einführung von Pflichten der Telekommunikationsanbieter zur Bevorratung oder Zugänglichmachung entsprechender Informationen nicht grundsätzlich entgegen. Zu entsprechenden Auseinandersetzungen zwischen Microsoft und der US-Regierung hinsichtlich der auf Firmenservern in Irland gespeicherten Daten: *M. Apuzzo/D. E. Sanger/M. S. Schmidt* Apple and Other Tech Companies Tangle With U.S. Over Data Access, New York Times v. 7.9.2015, http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=0.

[137] Beispielhaft: BVerfGE 49, 24 (56 f., Rn. 115 ff.) – Kontaktsperre; BVerfGE 115, 320 (346, Rn. 91) – Rasterfahndung II; BVerfGE 120, 274 (319, Rn. 220) – Online-Durchsuchung. Vgl. auch Österreichischer VfGH v. 27.6.2014, Az. G 47/2012-49 u.a., Rn. 168.

Tabuzonen. Eine gegenüber staatlichen Zugriffen vollständig abgeschirmte elektronische Kommunikation und Aktion brächte aber unabweisbare und schwere Sicherheitsrisiken für Drittbetroffene wie für staatliche Einrichtungen mit sich. Schon heute ist das Internet eben nicht allein ein Raum gesteigerter staatlicher Informationszugriffe, sondern auch ein Raum, in dem es für manche leichter geworden ist, sich dem sicherheitsbehördlichen Zugriff zu entziehen.[138]

IV. Fazit

Die neue Technologie elektronischer Kommunikation und ihrer Überwachung verändert den Schutz der Privatheit fundamental. Sie ist heute in einem Maße gefährdet und korrumpiert, das – gemessen an den traditionellen Maßstäben des Bundesverfassungsgerichts – das Verdikt der Verfassungswidrigkeit verdiente. Der seinerseits verfassungsrechtlich geschützte Gebrauch der Freiheit in der Anwendung der neuen Kommunikationsmittel und die verfassungsrechtlich legitime staatliche Sicherheitsverantwortung machen aber Relativierungen der Privatheit jenseits traditioneller Verfassungserwartungen[139] unausweichlich. Dem demokratisch legitimierten Gesetzgeber steht hier ein größerer Spielraum zu als vielfach angenommen wird. Dennoch bleibt eine verfassungsrechtliche und verfassungsgerichtliche Grenzziehung zum Schutz der Privatheit weiter unabdingbar. Sie sollte vorrangig zentralen und bislang vernachlässigten staatlichen Zugriffen auf die Privatheit zu Teil werden, denen es an Transparenz, öffentlicher Kontrolle und normativer Begrenzung noch in verfassungsrechtlich inakzeptabler Weise mangelt.

---

[138] Vgl. dazu BVerfGE 125, 260 (Rn. 260) – Vorratsdatenspeicherung: „In einem Rechtsstaat darf auch das Internet keinen rechtsfreien Raum bilden." Diese einschränkenden verfassungsrechtlichen Überlegungen müssen nicht bedeuten, dass Technologie hinsichtlich der Einhegung staatlicher Informationszugriffe keine Rolle spielen kann oder spielen darf. Denkbar sind etwa mittlere Lösungen, die darauf hinausliefen, den sicherheitsbehördlichen Zugriff wenn nicht auszuschließen, so doch zu hemmen und die so möglicherweise eine Abkehr von der Strategie der massenhaften Informationserfassung nahelegten. Nicht ohne Grund verheißt die aktuell wohl bekannteste Verschlüsselungssoftware einschränkend auch nur „PGP – pretty good privacy". Nach Auskunft der Bundesregierung ist es dem BND grundsätzlich möglich entsprechende Verschlüsselungen zu überwinden, vgl. BT Drs. 17/9640, 3.

[139] Vgl. etwa *P. Häberle* Aussprache zu Grundrechtsschutz der Privatheit (o. Fn. 14), VVDStRL 70 (2010), 95.

Leitsätze des 1. Referenten über:

Verfassung in ausgewählten Teilrechtsordnungen: Konstitutionalisierung und Gegenbewegungen im Sicherheitsrecht

I. Von der verfassungsrechtlichen Dystopie zur Realitätsbeschreibung

(1) Auf dem Feld des staatlichen Informationszugriffs und Informationsgebrauchs trifft ein hoch ambitionierter verfassungsrechtlicher Begrenzungsanspruch auf eine Gegenbewegung, die diesen Anspruch massiv unterläuft und entwertet.

a. Der verfassungsrechtliche Anspruch

b. Die Realität elektronischer Kommunikation und ihrer Überwachung

(2) Die Realität der elektronischen Kommunikation und ihrer Überwachung entspricht der verfassungsgerichtlichen Dystopie des Volkszählungsurteils.

(3) Dieser Realität lässt sich durch Selbstbeschränkung und Verzicht nicht effektiv begegnen.

(4) Entsprechende staatliche Kommunikationsbeschränkungen brächten überdies Freiheitseinschränkungen mit sich, die verfassungsrechtlich nicht zu rechtfertigen wären.

c. Reaktionen

(5) Die Reaktionen auf die fundamental veränderte Lage der Privatheit oszillieren zwischen einer fundamentalen Relativierung des menschenrechtlichen Privatheitsanspruchs einerseits und der verfassungsrechtlichen Forderung nach einem substantiell nachgesteuerten Privatsphärenschutz andererseits.

d. Ursachen

1. Entgrenzte Sicherheit?

(6) „Entgrenzte Sicherheit" gilt vielen als Ursache für die zugespitzte Spannungslage zwischen dem verfassungsrechtlichen Privatheitsanspruch und dem staatlichen Informationszugriff.

(7) Zu den Phänomenen entgrenzter Sicherheit zählen die Ergänzung des Strafrechts um weit gefasste Vorfeldtatbestände, die Auflösung des Gefahrenbegriffs, die Erweiterung der Adressaten sicherheitsbehördlicher Maßnahmen, die zu Tage tretenden Grenzziehungsschwächen der Verhältnismäßigkeit, neue fließende Übergänge von Repression und Prävention und der immer weiter ausgebaute Präventionsanspruch, die Zusammenarbeit von Polizei und Nachrichtendiensten und die Auflösung der ehemals territorialen Grenzen der sicherheitsbehördlichen Tätigkeit.

(8) Die allermeisten dieser Entgrenzungen bedingen zugleich eine Ausweitung des sicherheitsstaatlichen Zugriffs auf die private Kommunikation.

2. Technologischer Wandel

(9) Von ungleich größerer Relevanz ist der technologische Wandel, auf den die neue Sicherheitspolitik aufsattelt.

(10) Dieser Wandel erlaubt Strategien weitgehender Überwachung, die auch von deutschen Behörden verfolgt werden.

(11) Aus sicherheitspolitischer Sicht ist der technologische Wandel ein janusköpfiger.

II. Verfassungsgerichtliche Rahmensetzung

a. Bundesverfassungsgericht

(12) In der sicherheitspolitischen Debatte gilt das Bundesverfassungsgericht als „Champion" der bürgerlichen Freiheitsrechte, der einen überzogenen Sicherheitsanspruch von Exekutive und Legislative regelmäßig in seine verfassungsmäßigen Schranken weist.

(13) Eine genauere Analyse der inhaltlich anspruchsvollen Rechtsprechung des Bundesverfassungsgerichts vermittelt ein differenzierteres Bild eines zu Recht durchgängig nur relativen und gegenüber sicherheitspolitischen Erfordernissen abwägungsoffenen Schutzes der Privatsphäre.

(14) Problematisch ist der dogmatische Ausgangspunkt der Rechtsprechung des Bundesverfassungsgerichts, das von ihm selbst aus dem allgemeinen Persönlichkeitsrecht entwickelte Recht auf informationelle

Selbstbestimmung. Für die Grenzziehung im Bereich des staatlichen Informationszugriffs erschiene eine unmittelbar auf den Schutz der Privatheit abzielende Konzeption nicht nur konstruktiv überlegen, sondern auch mit Blick auf ihre potentiellen Ergebnisse und ihre europäische und internationale Anschlussfähigkeit vorzugswürdig. Problematisch erscheint die informationelle Selbstbestimmung auch deshalb, weil sie jedenfalls von ihrem konstruktiven Ausgangspunkt her kaum eine sinnvolle Unterscheidung zwischen öffentlicher und privater Sphäre erlaubt.

(15) Traditionelle Blindstellen kennt die Rechtsprechung des Bundesverfassungsgerichts im Umgang mit der Informationserhebung durch die Nachrichtendienste.

b. Europäische Verfassungsgerichte

(16) Die Rechtsprechung des EuGH zum Schutz der Privatheit erscheint inhaltlich vielversprechend.

(17) Manche ihrer kompetenzrechtlichen Prämissen sind mit der EU-Rechtsordnung aber unvereinbar.

III. Neue verfassungsrechtliche Grenzsteine

a. Verfassung als Rahmenordnung

(18) Fragen des Ausgleichs von Freiheit und Sicherheit sind der Sache nach regelmäßig politischer Natur und damit weithin dem demokratischen Entscheidungsprozess überantwortet.

b. Die Deprivilegierung der Geheimdienste

(19) Die traditionelle sicherheitsrechtliche Privilegierung der Nachrichtendienste überzeugt nicht.

(20) Aus verfassungsrechtlicher Sicht besteht hier ein substantieller normativer Nachholbedarf, der gegenüber den eher punktuell erforderlichen weiteren verfassungsrechtlichen Korrekturen des informationellen Handelns der sonstigen Sicherheitsbehörden vorrangig anzugehen ist.

c. Transparenz und Kontrolle

(21) Zu den strukturellen verfassungsrechtlichen Antworten auf die in jüngerer Zeit bekanntgewordenen staatlichen Informationszugriffe muss eine verstärkte Verpflichtung zur Transparenz des Handelns auch der Geheimdienste gehören.

(22) Allgemeine, aggregierte Informationen über Art und Ausmaß der geheimdienstlichen Informationszugriffe müssen deshalb künftig weit mehr als bislang aus der Geheimhaltung herausgenommen und damit öffentlich diskutiert werden.

(23) Die NSA-BND-Selektorenliste unterliegt dem parlamentarischen Untersuchungsrecht.

(24) Bei Entscheidungen zur Kontrolle der sachlichen Legitimation eines exekutiven Geheimhaltungsverlangens muss das Bundesverfassungsgericht die einschlägigen Dokumente gegebenenfalls selbst kritisch durch eine eigene „in-camera"-Betrachtung prüfen.

d. Verrechtlichung geheimdienstlichen Handelns

(25) Die Tätigkeit der Geheimdienste bedarf einer nachholenden Verrechtlichung durch Ermächtigungsnormen, die die tatbestandlichen Voraussetzungen und Grenzen des nachrichtendienstlichen Handelns – in der Sprache des Bundesverfassungsgerichts – „normenklar" bestimmen.

(26) Die als „Weltraumtheorie" bekannte Auffassung der Bundesregierung von der weitgehenden Schutzlosigkeit von Ausländern gegenüber dem Informationszugriff deutscher Behörden ist mit Art. 10 GG nicht vereinbar.

e. Grenzen der Informationserhebung und -verwendung

(27) Eine verfassungsrechtlich hinreichend bestimmte Grenzziehung fehlt der Informationserhebung und Informationsverwendung durch die Nachrichtendienste ganz allgemein.

f. Technologische Antworten und ihre rechtlichen Grenzen

(29) Verfassungsrechtliche Grenzziehungen des staatlichen Informationszugriffs werden durch zukünftige Entwicklungen der Verschlüsselungstechnik kaum entbehrlich werden. Entsprechende staatliche Einschränkungen sind verfassungsrechtlich grundsätzlich zulässig.

IV. Fazit

(30) Die neue Technologie elektronischer Kommunikation macht Relativierungen der Privatheit jenseits traditioneller Verfassungserwartungen unausweichlich. Dem demokratisch legitimierten Gesetzgeber steht hier ein größerer Spielraum zu, als vielfach angenommen wird. Die Grenzziehung zum Schutz der Privatheit sollte vorrangig solchen staatlichen Zu-

griffen gelten, denen es an Transparenz, öffentlicher Kontrolle und normativer Begrenzung noch in verfassungsrechtlich inakzeptabler Weise mangelt.