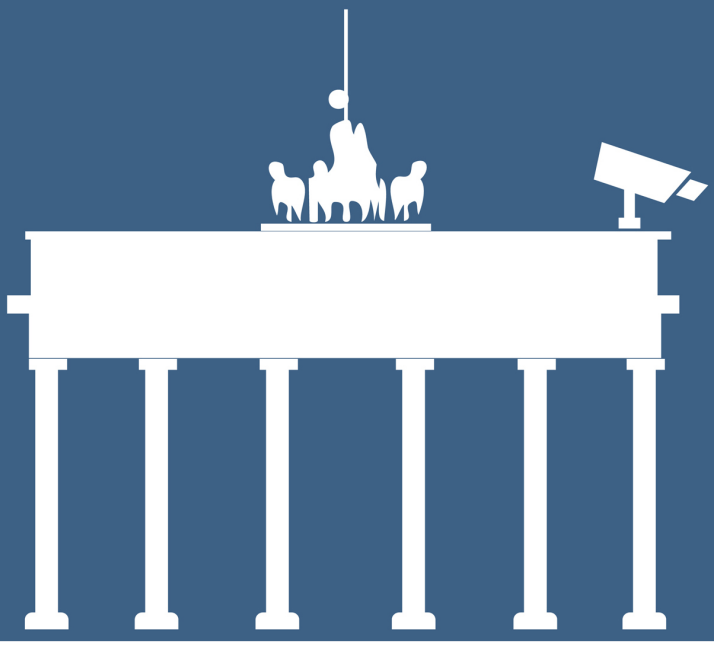
§ Telemedicus

Sommerkonferenz



Überwachung und Recht

HÄRTING

Internet & Gesellschaft Co:llaboratory

HUMBOLDT LAW CLINIC INTERNETRECHT

Telemedicus e.V. (Hrsg.)

Überwachung und Recht
Tagungsband zur Telemedicus Sommerkonferenz 2014

Telemedicus-Schriftenreihe
Band 1

Impressum
Verlag: epubli GmbH, Berlin
www.epubli.de

Alle Fundstellen, soweit sie ins Internet verweisen, wurden zuletzt überprüft am 05.11.2014.

Vorwort

In den vergangenen Jahren hat sich ein schleichender Wandel vollzogen: Der Schutz persönlicher Daten ist in der Mitte der Gesellschaft angelangt. Während Datenschutz noch vor wenigen Jahren weitgehend ein Nischenthema für Experten war, sind heute breite Teile der deutschen und europäischen Öffentlichkeit für den Schutz ihrer persönlichen Daten sensibilisiert – auch, aber nicht nur wegen der Enthüllungen von Edward Snowden.

„Überwachung und Recht" ist also ein Thema am Puls der Zeit, die Rechtsfragen um staatliche und private Überwachung die vielleicht drängendsten der letzten Jahre. Und doch stehen viele Diskurse noch ganz am Anfang. Um die Rechtsfragen systematisch aufzuarbeiten, konkrete und abstrakte Probleme anzugehen und erste Lösungsansätze zu diskutieren, haben wir die erste öffentliche Telemedicus Sommerkonferenz 2014 diesem Thema gewidmet. Große Ziele, die die Speaker wie Teilnehmer der Konferenz jedoch voll erfüllt haben. Wir freuen uns sehr, auf eine erhellende, produktive und auch unterhaltsame Telemedicus Sommerkonferenz 2014 zurückblicken zu können.

Dieser Tagungsband soll die wichtigsten Beiträge und Ergebnisse zusammenfassen. Damit unsere Erkenntnisse möglichst vielen Menschen zugänglich gemacht werden können, haben wir uns bewusst dafür entschieden, das Werk in primär digitaler Version und unter einer freien Lizenz zu veröffentlichen – in der Hoffnung, damit weitere Diskussionen anstoßen und bereichern zu können.

Wir bedanken uns herzlich bei allen Teilnehmern und Speakern der Telemedicus Sommerkonferenz für spannende Diskussionen und wertvolle Impulse und ganz besonders bei den Autoren, die uns für diesen Tagungsband ihre Beiträge zur Verfügung stellen. Außerdem danken wir dem Internet und Gesellschaft Collaboratory, der Humboldt Law Clinic Internetrecht, der Kanzlei HÄRTING

und der gemeinnützigen Hertie Stiftung, ohne die weder die Sommerkonferenz noch dieser Tagungsband möglich gewesen wären.

Adrian Schneider, Vorstand Telemedicus e.V.

Inhaltsverzeichnis

Überwachung, Datenschutz und die Zukunft des Informationsrechts

Kai von Lewinski

„Überwachung" und „Recht", also „Datenschutzrecht" – dieses Themen-Duo verspricht Spannung, denn gegensätzlicher geht es kaum. „Überwachung" ist das Schlechte, „Datenschutz" etwas bald schon absolut Gutes – jedenfalls wenn man die Hohepriester des Datenschutzrechts die Bergpredigt des Volkszählungsurteils[1] (und nun auch einiger EuGH-Entscheidungen) wie eine Monstranz vor sich hertragen sieht. Und Gläubige des „Super-Grundrechts auf Sicherheit"[2] sehen die Sache genau andersherum.

Beide gläubige Gewissheiten sollen im Folgenden relativiert werden. Dabei mögen Wissenschaftler die „Hofnarren der modernen Gesellschaft"[3] sein, sie sind aber nicht auch der Geist, der stets verneint. Und so sollen auch konstruktiv die rechtspolitischen Richtungen aufgezeigt werden, in die sich Überwachungsbegrenzung jenseits des überkommenen Datenschutzes entwickeln kann. Der Beitrag wird sich zunächst mit dem Umstand der Überwachung auseinandersetzen (1), dann mit der überholten Konzeption des Datenschutzrechts (2). Beides soll eher relativiert werden. Anschließen werden sich einige Gedanken zu rechtlichen Begrenzung von Überwachung und Datenmacht gemacht (3). Am Ende (4) wird freilich kein ab- und umschließendes rechtli-

[1] So schon ketzerisch *Meister* DuD 1986, S. 173, 175; s.a. *v. Lewinski*, in: *Auernhammer*, BDSG, 4. Aufl. 2014, Einl. Rn. 27.
[2] So prominent der damalige Bundesinnenminister *Friedrich*; kritisch dazu die damalige Bundesjustizministerin *Leutheusser-Schnarrenberger* MMR 2013, 481ff.; zur rechtdogmatischen Einordnung des „Grundrechts auf Sicherheit" *v. Lewinski*, in: *Auernhammer* (Fn. 1), Einl. Rn. 67.
[3] *Dahrendorf*, Gesellschaft und Demokratie in Deutschland (Tb.), 5. Auflage 1977, S. 306 f.

ches Konzept zur Beschreibung und Bewältigung der Fragen der Informations- und Überwachungsgesellschaft stehen. Der Zustand des heutigen Informationsrechts, das wir bislang bestenfalls fragmentarisch überblicken, lässt noch nichts anderes zu.

1 Überwachung als Befund und Ausgangspunkt

1.1 Überwachung als Kontrolle der Umwelt

„Überwachung" ist seit einiger Zeit negativ konnotiert[4]. Dabei ist Überwachung als gezielte Beobachtung der dinglichen und sozialen Umwelt eine natürliche Verhaltensweise. Sie ist also nicht nur inhaltlich und moralisch neutral, sondern in Gestalt der Neugier menschlich und kreatürlich[5]. Auch ist Überwachung in vielen Konstellationen etwas, das gesellschaftlich gewünscht und sogar von Rechts wegen angeordnet wird:[6]

- Das Baby-Fon ist eine technische Wanze, ohne die Eltern vom gesellschaftlichen Leben und Familienfeiern ausgeschlossen wären.
- Die Berg*wacht* und Wasser*wacht* sind ein wichtiger Teil der Tourismusinfrastruktur.
- Der TÜV, der die Überwachung im Namen trägt („Technischer Überwachungsverein"), ist für die Sicherheit auf Deutschlands Straßen unverzichtbar.
- Und jeder Rechtsanwalt kennt die Wiedereinsetzung in der vorigen Stand (§§ 233 ff. ZPO; § 44 StPO; § 60 VwGO; § 32 VwVfG; § 67 SGG; § 56 FGO;

[4] Ausdrücklich Wikipedia, Art. „Überwachung", Abschn. „Überwachung von Objekten und Naturgefahren", http://de.wikipedia.org/wiki/%C3%9Cberwachung#.C3.9Cberwachung_von_Objekten_und_Naturgefahren.
[5] Auf die besondere militärische Bedeutung der Überwachung (Aufklärung) für die Sicherheit weist *Bendrath* APuZ 18–19/2014, S. 20, 20, hin.
[6] Dazu auch *Dalby*, in diesem Band ab S. 83.

§ 93 Abs. 2 BVerfGG), die einen „hinreichend geschulten, eingewiesenen und *überwachten*“ Mitarbeiter voraussetzt.[7]

So ist es nicht verwunderlich, dass Synonyme des Wortes „Überwachung“ wie „Aufsicht“, „Monitoring“, „Kontrolle“ oder „Supervision“ nicht ganz so negative Gefühle hervorrufen.

1.2 Überwachungsgefühl ist zeitgebunden

Abseits von der linguistischen Ambivalenz der „Überwachung“ ist sie auch in hohem Maße zeitgebunden. Überwachung ist nicht immer dasselbe gewesen und wird auch in Zukunft anders empfunden werden als heute.

1.2.1 Heutige großstädtische Anonymität

Unser Gefühl von Freiheit, Beobachtetsein und Überwachung ist das des 20. Jahrhunderts. Es ist die Metropole *Georg Simmels*, deren Freiheitsgefühl auf Anonymität aufbaut,[8] das für die heutige Gesellschaft prägend ist[9] – komme man nun aus Berlin-Charlottenburg oder aus Passau-Hacklberg. Die moderne Gesellschaft ist insoweit eine Stadtgesellschaft. Auch das „globale Dorf“[10] des Internets ist nicht durch eine dörflich-familiäre Atmosphäre gekennzeichnet, sondern (nur) durch die jederzeitige Erreichbarkeit von Attraktionen, wie sie

[7] *v. Lewinski*, Anwaltliches Berufsrecht, 3. Aufl. 2012, S. 110; illustrierende Beispiele bei *Hartmann*, in: *Baumbach/Lauterbach/Albers/Hartmann*, ZPO, 71. Aufl. 2013, § 233 ZPO Rn. 146–153.
[8] Vgl. dazu insb. *Simmel*, in: *Petermann* (Hrsg.), Die Großstadt (Jahrbuch der Gehe-Stiftung Dresden Bd. 9), Dresden 1903, S. 185–206.
[9] Die heutige Großstadt als „Panoptikon“ i.S. *Foucaults* interpretierend *Bendrath* APuZ 18–19/2014, S. 20, 20.
[10] Der Begriff stammt von dem Medienwissenschaftler *Marshall McLuhan*, der ihn (wohl) zuerst in „The Gutenberg Galaxy“ (1962; dt.: Die Gutenberg-Galaxis) verwendete und (zusammen mit *B.R. Powers*) in „The Global Village“ (1992; dt. Ausgabe 1995) vertiefte.

eher für verdichtete Stadtviertel steht. – „Digitaler Kiez“ wäre also eigentlich passender.

1.2.2 Mittelalterliche Vogelfreiheit als Verlust sozialer Einbindung

Das heutige in Stadt und Land gleichermaßen städtische Lebensgefühl wäre dem mittelalterlichen Menschen kaum verständlich gewesen; vor allem hätte er sich wohl auch nicht wohlgefühlt. Das Mittelalter war nicht nur sehr viel dörflicher geprägt, sondern auch durch personale Herrschaftsverbände (Lehnswesen, Grundherrschaft). Man war Mensch als soziales Wesen nur in der (engen) Einbindung in Personenverbände. Zwar gab es zu der Zeit keinen (absolut) Großen Bruder, immer aber einen (relativ) größeren Bruder, daneben aber auch (relativ) kleinere Brüder und Schwestern. Die heutige simmel’sche Freiheit in der Großstadt, die Möglichkeit der Selbstverwirklichung der schwäbischen Pfarrerstöchter in Kreuzberg durch die Ablösung vom Elternhaus, war damals in Gestalt der Vogelfreiheit[11] der gesellschaftliche und meist kurz darauf auch der physische Tod.

1.2.3 Panoptismus

Das in Sachen Herrschaftsausübung „persönliche“ und daher eher zupackend-derbe Mittelalter wurde von dem neuzeitlich-modernen entpersonalisierten Staat und seiner Bürokratie abgelöst. Der französische Philosoph *Michel Foucault* (1926–1984) hat als prägendes Moment unserer Epoche überhaupt die Überwachung angesehen. Den Begriff des Panoptismus, den er für die umfassende Überwachung und Kontrolle in seinem Werk „Überwachen und

[11] Dabei ist es unerheblich, dass der Begriff der Vogelfreiheit ursprünglich im Mittelalter noch nicht mit der juristischen Ächtung (Acht) verbunden war (*Schmidt-Wiegand*, Art. „Vogelfrei“, in: Handwörterbuch zur Deutschen Rechtsgeschichte, Bd. 5 1998, Sp. 930–932). Denn eine individualistische Existenz war damals kaum denkbar und möglich.

Strafen“ (1976; frz. „Surveiller et punir“, 1975) prägte, war angelehnt an das Gefängnismodell des Panopticons von *Jeremy Bentham* (1748–1832)[12], wie es sich etwa in dem Untersuchungsgefängnis in Moabit materialisiert hat. Unmittelbare und körperlich wirkende Gewalt sei mit der Zeit immer stärker „verinnerlicht“ und durch die Beobachtung bzw. die Illusion des Beobachtetwerdens ersetzt worden. Insoweit ist die moderne arbeitsteilige und komplexe Welt wohl notwendig panoptisch, weil die vielen sozialen und wirtschaftlichen Interaktionen und Interdependenzen flächendeckend gar nicht mehr hoheitlich durchgesetzt werden könnten, ohne dass der (Recht-)Staat zugrundeginge.

1.2.4 Postpanoptisches Zeitalter und Post-Privacy

Teilweise wird die heutige Zeit auch als postpanoptisch bezeichnet, etwa von *Zygmunt Bauman* (geb. 1925) und dessen Werk „Flüchtige Moderne“ (2003; engl. Original: „Liquid Modernity“, 2000). Dies meint aber nicht das Ende der (verinnerlichten) Beobachtung, sondern (nur) die Ablösung territorial und durch direkte Beobachtung wirkender „panoptischer“ Überwachung durch elektronische und virtuelle Techniken. Postpanoptisch meint also nur den Beobachtungsmodus, nicht die Erscheinung selbst.

Eine mögliche Zukunft dieser Art ist die der Post-Privacy. Hier wird vor der Tatsache der Überwachung unverzagt kapituliert und unter Zurücklassung der foucault’schen Machtmechanismen fröhlich weitergelebt. Ob ein „Zeitalter nach dem Datenschutz“ tatsächlich kommt und es innerhalb und außerhalb der Datenschutzbehörden wünschbar wäre, wird sich weisen. – Dem soll hier auch nicht weiter nachgegangen werden.

[12] *Bendrath* APuZ 18–19/2014, S. 20, 20.

1.2.5 Überwachung als soziales Übergangsproblem

Für die Zwecke dieses Beitrags reicht es zu zeigen, dass der Mensch anpassungsfähig ist wie die Ratte, gerade auch an veränderte soziale und technische Umwelten. In einigen Generationen werden wir uns als Gesellschaft an eine elektronisch vernetzte Umwelt angepasst haben, wie immer die auch aussieht – so wie wir uns auch an den rechten Winkel, die Gleichheit der Menschen, die Schrift und das Buch, die Uhr und die Eisenbahn, den Tabak und sein Verschwinden[13] gewöhnt haben.

Das gegenwärtige und heutige Thema ist zwar von einer menschheitsgeschichtlichen Warte aus ein Übergangsthema. Technisch unterstützte Überwachung wird es wohl immer geben, sie ist aber vielleicht zukünftig kein relevantes Problem mehr. Für die jetzige Generation (und wahrscheinlich auch noch einige Folgegenerationen) ist es aber ein drängendes Thema. Das relativiert die Relativierung des Überwachungsproblems: Es ist der Beruf unserer Zeit (und wahrscheinlich auch noch der folgender Generationen), die Überwachung technisch und rechtlich einzuhegen.

1.3 Gefahren

Wenn also für eine Übergangszeit, die aber unser aller Lebenszeit sicherlich überschreiten wird, Überwachung als ein Problem empfunden wird, dann gilt es, dieses Problem genauer zu benennen:

Wie die Alltagserfahrung lehrt, wie die Kybernetik erklärt und wie das Bundesverfassungsgericht in der Volkszählungsentscheidung ausgeführt hat,[14] ändert

[13] Dazu zeitgeschichtlich *B. Hammer*, Rauchfreie Welt: Zwischenstation Zigarettenraucher, Telepolis v. 31.08.2014, http://heise.de/-2305123.
[14] Insb. *BVerfGE* 65, 1, 42 f. – *Volkszählung*: „Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über

sich das Verhalten von Menschen unter Beobachtung. Dies ist eine Folge sozialen Zusammenlebens, vielleicht sogar deren Voraussetzung. Entscheidend scheint mir, welche Folgen sich jeweils an ein beobachtetes oder beobachtbares Verhalten knüpfen. Je freier und toleranter eine Gesellschaft ist, desto unbefangener kann man sich auch unter Beobachtung bewegen und verhalten.[15]

Absolute Toleranz aber kann es nicht geben. Und auch wenn es sie gäbe, scheint es wünschenswert, den Einzelnen vor den Zudringlichkeiten auch einer sehr toleranten Umwelt zu schützen, ihm jedenfalls eine Rückzugsmöglichkeit zu bieten.

---

vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten."

[15] Allerdings gilt es als gesicherte kriminalistische Erkenntnis, dass öffentliche Videoüberwachung alleine keinen nennenswerten dauerhaften Rückgang der Delinquenz nach sich zieht; entscheidend ist die Veränderung realen Verfolgungsdrucks. Dies wirft die Frage auf, welche Auswirkung dieses gegen flächendeckende Videoüberwachung gerne und häufig vorgebrachte Argument dann auf die Überwachung der Gesellschaft hat.

2 Datenschutz als Leitkonzept des Informationsrechts?

Der Schutz vor Überwachung wird gemeinhin unter der Überschrift des Datenschutzes verhandelt. Das ist auf den ersten Blick durchaus plausibel. Allerdings zeigt sich bei näherem Hinschauen, dass das Datenschutzrecht, wie wir es in Deutschland seit nun über 40 Jahren kennen, zum einen überhaupt ein überprüfungs- und überholungsbedürftiges Konzept ist. Und zum anderen wird das konzeptionelle Potential des Datenschutzrechts überschätzt und überdehnt. Datenschutzrecht ist zwar ein wichtiger und in seinem Alter auch ehrwürdiger Pfeiler des Informationsrechts. Er ist aber kein informationsrechtlicher Alleskleber!

Damit soll keinesfalls der Datenschutz (als Schutzziel) relativiert werden, sondern nur der Datenschutz als dogmatisches und institutionelles System (als Schutzkonzept). Hiermit tun wir uns in Deutschland besonders schwer, weil mit dem Volkszählungsurteil eine ausgesprochen starke grundrechtliche Fundierung des Datenschutzes besteht. Auf europäischer Ebene haben wir inzwischen eine vergleichbar starke Zementierung des Datenschutzes, nicht nur in Art. 8 GRCh, sondern auch in Art. 16 AEUV.

Dabei spricht aber auch gar nichts gegen eine robuste grundrechtliche Absicherung von gefährdeten Grundrechten. Gerade aber an der Schwelle zur Informationsgesellschaft, deren Umrisse wir erst erahnen, scheint es jedenfalls reflektionsbedürftig,[16] die Einsichten und den Erkenntnisstand der späten Industriegesellschaft schon in Stein zu meißeln.

[16] Zum verfassungsrechtlichen Anpassungsbedarf über den Bereich der Grundrechte hinaus s.u., Abschnitt 3.4.

2.1 Datenschutzzentriertheit des Informationsrechts

Jedenfalls sollten wir unsere Ansprüche und Erwartungen an das Datenschutzrecht nicht überspannen.

So wie die Geschichtswissenschaft nicht (mehr) von einer universalen Weltgeschichte ausgeht, sondern von Vergangenheit*en,*[17] und die Technikwissenschaften nicht mehr eindimensional von „der Zukunft" sprechen, sondern mit dem Konzept der „Technik*zukünfte*" arbeiten,[18] so sollte sich auch das Informationsrecht aus der Eindimensionalität des Datenschutzrechts (und des Immaterialgüterrechts) lösen. Die Geschichtserzählung unserer Schulbücher ist nur für uns Europäer plausibel, die Informationsgesellschaft nur für diejenigen, die sich mit IT beschäftigen, und die informationelle Selbstbestimmung (als Konzept) nur für Datenschützer. So wie die Geschichtsschreibung den westlichen Eurozentrismus überwinden muss, muss das Informationsrecht sich aus der konzeptionellen Vorherrschaft des Datenschutzrechts lösen. Wir bleiben sonst in einer „Datenschutz-Filterblase" („Datenschutz-Bubble") sitzen.

2.1.1 Allgemeine Kritik am Konzept des Datenschutzes

2.1.1.1 Unbestimmtes Schutzgut

Eine allgemeine Kritik des Datenschutzrechts fängt damit an, dass das Schutzgut des Datenschutzrechts nur schwer zu definieren ist. Dass das Datenschutzrecht dem Datenschutz dient, ist offensichtlich zirkulär. Dass der Datenschutz nicht die Daten schützt, ist eine Binsenweisheit. Was der Datenschutz aber

[17] Siehe nur den jüngsten Vortrag von *Osterhammels* „Vergangenheiten – Über die Zeithorizonte der Geschichte" anlässlich des 60. Geburtstags der Bundeskanzlerin (gekürzt abgedr. in F.A.Z. v. 19.07.2014, S. 11.
[18] Siehe bspw. *Grunwald*, Technikzukünfte als Medium von Zukunftsdebatten und Technikgestaltung, 2012; acatech (Hrsg.), Technikzukünfte: Vorausdenken – Erstellen – Bewerten, 2012.

eigentlich will, ist gar nicht so einfach zu benennen. Oder anders gewendet: Es gibt viele (und unterschiedliche) Verständnisse über die Aufgabe des Datenschutzes und des Datenschutzrechts.

- Dient das Datenschutzrecht dem Individuum oder der Gesellschaft?[19] Für die individualistische Sichtweise spricht § 1 Abs. 1 BDSG und überhaupt die subjektive Schutzrichtung der Grundrechtsordnung. Aber ein Blick etwa auf § 1 Nr. 2 hessDSG zeigt, dass eine informationelle Gefahrenlage auch auf verfassungsrechtlicher Ebene zwischen den Staatsgewalten und Verfassungsorganen bestehen kann.
- Geschützt werden soll nach § 1 Abs. 1 BDSG das Persönlichkeitsrecht. Dies aber nicht nur vor Verletzungen, sondern auch schon vor (bloßen) Beeinträchtigungen. Wir haben es an dieser Stelle mit einer doppelten Unschärfe zu tun. Denn zum einen ist das (Allgemeine) Persönlichkeitsrecht als „entwicklungsoffenes" Grundrecht nicht abschließend und insoweit offen. Und der Schutz vor Beeinträchtigungen, also der Schutz des Vorfeldes von Verletzungen, ist jedenfalls dogmatisch ebenfalls noch nicht abschließend erfasst.
- Wenn man sich dem Persönlichkeitsrecht als Schutzgut zuwendet, dann erkennt man verschiedene Ausprägungen: Schützt das Datenschutzrecht die Autonomie[20] im Sinn von informationeller Selbstbestimmung? Oder im Sinn von informationeller Selbstbestimmtheit? Geht es um körperliche Zustände wie Scham?[21] Werden in diesem Vorfeld vielleicht doch physische[22],

[19] Zu einem „gesamtgesellschaftlichen Informationsgleichgewicht" *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 55 ff.
[20] *v. Lewinski* (Fn. 19), S. 20 f.
[21] *Krimphove*, Scham als Verhaltenssteuerung im Recht, RTheorie 43 (2012), S. 91–115.
[22] *v. Lewinski* (Fn. 19), S. 30 f.

soziale[23] oder logische[24] Räume geschützt, obwohl Datenschützer gerne den Abschied von dem Sphärenmodell verkünden?

- Geht es um Abbildschutz? Die Bestimmungsmacht über das informationelle Abbild seiner selbst in dem Kopf und Rechner eines anderen? Der Begriff von der „informationellen Selbstbestimmung" ist insoweit irreführend, weil er das Ziel der (Selbst-)Bestimmung über das eigene Außenbild mit dem Mittel der Bestimmung und Beschränkung von Datenbeständen bei *Dritten* gleichsetzt, es sich mithin um „informationelle Fremdbestimmung" oder „informationelle Fremdbeschränkung" handelt.[25]
- Vielleicht geht es eigentlich auch nicht um die kleinteilige Regelung der Verarbeitung von personenbezogenen Daten, sondern um etwas Größeres wie die Verhinderung von Persönlichkeitsprofilen?[26]
- Noch wenig diskutiert wird der Datenschutz im Kontext der Anti-Diskriminierung.[27] Beide Bereiche scheinen auf den ersten Blick – jedenfalls von der Dogmatik des Informationsrechts her – nicht viel miteinander zu tun zu haben. Gemeinsam ist aber beider Ziel, vorhandene Informationen über eine Person aus dem Prozess der Bewertung und des Urteils herauszuhalten. Datenschutz und Anti-Diskriminierung adressieren nicht unmittelbar oder jedenfalls nicht zentral den Akt der Überwachung selbst. Sie

---

[23] *v. Lewinski* (Fn. 19), S. 35 ff.; zum Sphärenmodell *Di Fabio*, in: *Maunz/Dürig*, Grundgesetz Kommentar, 70. EGL 2013, Art. 2 GG Rn. 158*; Barrot,* Der Kernbereich privater Lebensgestaltung, 2012, S. 29 ff.

[24] Das *BVerfG* erweiterte im Jahr 2008 mit seiner Entscheidung *BVerfGE* 120, 274 ff. – *Onlinedurchsuchung* den Schutz logischer Räume.

[25] Zu diesem Konzept *v. Lewinski* (Fn. 19), S. 40 ff.

[26] Zur Bildung von Persönlichkeitsprofilen in der Kreditwirtschaft *Klein* BKR 2003, 488, 489; zum Handel mit Persönlichkeitsprofilen *Moos* MMR 2006, 718 ff.

[27] Zur Verbindung von Datenschutz und Anti-Diskriminierung *v. Lewinski*, (Fn. 19), S. 46; vgl. auch *Thüsing*, in: Münchener Kommentar zum BGB, 6. Auflage 2012, § 1 AGG, Rn. 38, § 11 AGG, Rn. 17; umfassend zu verfassungsrechtlichen Aspekten des AGG *Dittmann*, Privat-rechtliche Diskriminierungsverbote aus verfassungsrechtlicher Sicht, 2010, insb. S. 86 et pass.

machen aber im Sinne eines – untechnisch gesprochen – Verwertungsverbots die Überwachung sinnlos.

2.1.1.2 Unscharfer Anwendungsbereich in Zeiten von Big Data

Wenn in den Zeiten von Big Data in immer mehr Kontexten die Anonymität in Datenbeständen nicht mehr gewährleistet werden kann, eine Personen*beziehbarkeit* also besteht und damit der Anwendungsbereich des Datenschutzrechts eröffnet ist, wird das herkömmliche Datenschutzrecht überdehnt. Im Einzelfall ist die Ausdehnung des Datenschutzrechts auf wahrscheinlichkeitsbasierte Sachverhalte (Scoring, Mikrodemographie) vielleicht angemessen; gesamthaft aber werden damit Rechtsregeln auf einen Bereich übertragen, der nach der ursprünglichen Konstellation gerade das Komplementärstück zur personenbezogenen Datenverarbeitung war. Wenn das Datenschutzrecht diesen Schritt machen will oder soll, muss es zu einem allgemeinen Datenrecht oder Informationsrecht werden.

2.1.1.3 Überzeitliche Gültigkeit des Konzepts?

Das (deutsche) Konzept des Datenschutzes, das der „Informationellen Selbstbestimmung", ist bald fünfzig Jahre alt und entstand vor dem Hintergrund einer Welt der Großrechner von der Rechenkapazität eines besseren Smartphones. Dieser Ansatz zur Regelung der Informationsgesellschaft hat so viel empirische Evidenz und Plausibilität wie die ersten (preußischen) Dampfkessel-Regularien für das heutige Umweltrecht.[28] Diese Einschätzung scheint auch in der Bundesregierung geteilt zu werden, wenn etwa der Bundesinnenminister *de Maizière*

[28] Zur gleichwohl bestehenden Bedeutung der (systematisch arbeitsschutzrechtlichen) preußischen Dampfkesselgesetzgebung für das heutige Immissionsschutzrecht *Kloepfer*, Umweltrecht, 3. Aufl. 2004, § 2 Rn. 27 ff.

meint, „unser liebevoll gestricktes deutsches Datenschutzrecht“ habe ausgedient.[29]

2.1.1.4 Verrechtlichungsfalle und Normenflut

Sicherlich ursprünglich ungeplant sitzt das Datenschutzrecht in einer Verrechtlichungsfalle, die es sich selbst gestellt hat.[30] Denn durch das Verbotsprinzip (§ 4 Abs. 1 BDSG) und die grundrechtshohe Aufhängung der informationellen Selbstbestimmung bedarf jede noch so triviale personenbezogene Datenverarbeitung eines Erlaubnistatbestands. Und die von der Verwaltung gewünschten und die von der Wirtschaft essentiell benötigten Erlaubnistatbestände hat der Gesetzgeber dann in den letzten Jahrzehnten auch geschaffen. Dass er hierfür auf weitreichende Generalklauseln, insb. § 28 Abs. 1 S. 1 Nr. 2 BDSG und die Regelungen der §§ 13 ff. BDSG bzw. entsprechender landesdatenschutzrechtlicher Regelungen, zurückgreift, sei hier nur angemerkt.

2.1.1.5 Defensives Risikorecht

Das prägende Regelungsprinzip des (deutschen) Datenschutzrechts ist das Verbot mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG). Über das Für und Wider dieser Regelungstechnik und die Frage, ob es sich dabei sogar um ein materielles Regelungsprinzip handelt, ist viel geschrieben worden. Unabhängig davon ist auch ohne Blick in die Entstehungsgeschichte festzustellen, dass dieser datenschutzrechtliche Regelungsansatz einer des Risikorechts ist. Und der gewählte risikorechtliche Ansatz ist eher der der Risikobegrenzung als der der Chancenermöglichung. Man muss in diesem Zusammenhang nicht von Technikfeindlichkeit des Datenschutzrechts sprechen,[31] aber der Regelungsansatz

[29] Bundesinnenminister *de Maizière*, Das Netz – Raum der Chancen und der Freiheit, F.A.Z. v. 18.08.2014, S. 6.
[30] *v. Lewinski*, in: *Auernhammer* (Fn. 1), Einl., Rn. 107 m.w.N.
[31] Vgl. dazu aber die Parallele, die *de Maizière*, Das Netz – Raum der Chancen und der Freiheit, F.A.Z. v. 18.08.2014, S. 6, zum Eisenbahnwesen zieht, das sich nicht auf den heutigen Stand entwickelt hätte, wenn zu Beginn zum Schutz der

betont eher die Risiken als die Chancen – ganz anders übrigens als das Informations*freiheits*recht.

2.1.1.6 Datenschutz als Vorfeldschutz

Ein weiteres risikorechtliches Merkmal ist die Vorfeldschutzkaskade, also die mehrfache Vorverlegung des Persönlichkeitsrechtsschutzes.[32] Wie Matrjoschka-Puppen umhüllen mehrere Schutzschichten das verletzliche Innere des Menschen. Dieser Ansatz des Vorfeldschutzes hat den Nachteil, dass jede Verlagerung in das Vorfeld den Schutz des eigentlichen Schutzgutes unscharf werden lässt. Überschießender Schutz, der unter Verhältnismäßigkeitsgesichtspunkten problematisch ist, Schutzlücken und sogar Dysfunktionalitäten sind die Folge.[33]

2.1.2 Defizite bei der Beschreibung von Überwachung

Die eben skizzierten allgemeinen Schwächen des Datenschutzrechts sind teilweise unmittelbar im Überwachungskontext relevant.

2.1.2.1 Keine Regelung des Scheins der Überwachung

Da das Datenschutzrecht die (tatsächliche) personenbezogene Datenverarbeitung zur Voraussetzung hat, gilt es nicht für den bloßen Schein einer Datenverarbeitung. Sinnfälliges Beispiel hierfür sind Kameraattrappen.[34] Vom Datenschutz erfasst ist nur die *tatsächliche Überwachung*, während die psychische Beeinträchtigung von dem *Gefühl der Beobachtung* ausgeht.

Kühe vor den „vorbeirauschenden" Zügen eine Geschwindigkeitsbeschränkung eingeführt worden wäre.

[32] Zur Vorfeldschutz-Kaskade im Datenschutz *v. Lewinski* (Fn. 19), S. 82 f.

[33] Ausführlich *v. Lewinski* (Fn. 19), S. 83–85.

[34] H.M., z. B. *Scholz*, in: *Simitis*, BDSG, 8. Aufl. 2014, § 6b Rn. 28.

2.1.2.2 Unzureichende Regelung von Algorithmen

Ein weiterer Mangel ergibt sich daraus, dass Regelungsgegenstand des Datenschutzrechts Daten als solche sind und Algorithmen nur unzureichend erfasst werden.[35] Das BDSG enthält keinerlei explizite oder differenzierte Regelung zu Algorithmen; § 6a BDSG kann lediglich als Regelungsversuch angesehen werden. Die Vorschrift soll verhindern, dass der Mensch zum Objekt automatisierter Entscheidungen gemacht wird.[36] Algorithmen werden jedoch weder explizit noch direkt geregelt. Vielmehr stellt § 6a BDSG eine indirekte Regelung von Algorithmen durch materielle und verfahrensmäßige Vorgaben dar.

2.1.2.3 Eindimensionalität

In einer vom Individuum und dem Persönlichkeitsrecht losgelösten Betrachtung der Überwachungsfrage zeigt sich ein weiterer Mangel: Das (deutsche) Datenschutzrecht schützt nur natürliche Personen, nicht also auch Unternehmen und Vereine.[37] Aber auch diese verhalten sich unter Beobachtung anders, wie jeder Außenprüfer eines Finanzamts bestätigen kann. Natürlich haben juristische Personen andere Rationalitäten als Menschen; die Verhaltensänderung unter Beobachtung, wenn man sie gesamtgesellschaftlich problematisiert, tritt aber auch hier auf.

Ebenfalls nicht vom Datenschutzrecht erfasst ist die Überwachung im familiären und persönlichen Bereich. Wegen der (grundrechtlich wohl notwendigen) sogenannten „Haushaltsausnahme“ des § 1 Abs. 2 Nr. 3 a.E. BDSG ist der private

---

[35] Ähnlich *Lanier*, Googles Datenmacht, Wer die Daten hat, bestimmt unser Schicksal, F.A.Z. online vom 24.04.2014, http://www.faz.net/aktuell/feuilleton/debatten/googles-datenmacht-wer-die-daten-hat-bestimmt-unser-schicksal-12907065.html.

[36] *v. Lewinski*, in: *Wolff/Brink*, BeckOKDatenschutzR, 9. Ed. 2014, § 6a BDSG Rn. 1.

[37] *v. Lewinski* (Fn. 19), S. 8 ff.: Datenschutz betrifft nur die Konstellation („Schutzrichtung“) Individuum–Institution (Unternehmen bzw. Verwaltung), nicht auch die von Institution–Institution; siehe auch *Dammann*, in: *Simitis* (Fn. 34), § 3 Rn 17.

Bereich zwischenmenschlicher Beziehungen ebenfalls vom Datenschutzrecht ausgenommen. Dass hier die perfidesten Überwachungen und die tiefsten Kränkungen geschehen, zeigt der Blick in fast jedes beliebige Fernseh- und Theaterdrama.

Einen Grenzfall wird in der zuletzt diskutierten Dashcam-Entscheidung des VG Ansbach beschrieben.[38] Die private Videoaufnahme fällt nicht in den Anwendungsbereich des BDSG, ist aber doch ein verbreitetes Phänomen, so dass Richter hier Regelungs- und Handlungsbedarf sahen.

2.1.3 Zunehmende Antiquiertheit des Datenschutzrechts

Das „Recht auf informationelle Selbstbestimmung", wie es seine Ausprägung im Datenschutzrecht gefunden hat, ist also nur bedingt geeignet, die Fragen der „überwachten Gesellschaft" zu adressieren. Nun ist es natürlich einfach, das BDSG zu beschimpfen, nur weil ein Gesetz aus dem Industriezeitalter die Probleme des Informationszeitalters nicht in jeder Hinsicht adäquat anspricht und löst. Schwerer ist es, ein besser passendes informationsrechtliches Modell zu präsentieren. Hier befindet sich die Wissenschaft noch sehr am Anfang.

2.2 Grundprinzip des Informationsrechts?

Über die Erkenntnis, dass es bei Kommunikation in einer Gesellschaft auf das Zusammenspiel von Geheimhaltung und Offenheit ankommt und dass es ein rechtliches Prinzip der „Informationsgerechtigkeit"[39] geben müsse, sind wir dabei noch nicht hinausgekommen. Bemerkenswerterweise können wir Juris-

[38] *VG Ansbach*, Urt. v. 12.08.2014, Az. AN 4 K 13.01634.
[39] *Kloepfer*, Informationsrecht, 2002, § 4 Rn. 15 ff.

ten noch nicht einmal den Unterschied zwischen Daten, Information und Wissen allgemeingültig definieren.[40]

2.2.1 Beschränkung oder Freiheit von Information

„Freiheit von Information" hat eine hohe Suggestivkraft. Die auch politisch-programmatische Benennung der Informationszugangsgesetze als „Informations*freiheits*gesetze" und das studentische und anti-reaktionäre „Die Gedanken sind frei …" machen dies unmittelbar plausibel. Ob es sich bei der Freiheit von Information allerdings um ein allgemeines Prinzip oder gar ein Axiom des Informationsrechts handelt, muss einstweilen mit einem Fragezeichen versehen werden. Wir können nicht einmal sagen, ob die Beschränkung von Information oder deren Freiheit die rechtliche Grundannahme der Informationsgesellschaft ist; vermutlich können dies nicht einmal die Beauftragten für den Datenschutz *und* den Informationszugang – und wenn sie es könnten, könnten sie ihr Amt nicht mehr gescheit ausüben… Illustriert werden kann diese Unsicherheit über den informationsrechtlichen Ausgangspunkt mit der (kurzen) Kontroverse zwischen *Thomas Giesen*[41] und *Stefan Brink*[42] über die Frage, wem die personenbezogenen Daten gehören.

Was man aber sagen kann, ist, dass der natürliche Zustand von Information der der Unbegrenztheit ist. Ob man hieraus ein rechtliches Grundprinzip der Freiheit folgern kann oder – im Gegenteil – der Grundton des Informationsrechts gerade die Begrenzung der natürlichen Freiheit sein muss, ist die große rechtspolitische Frage der Informationsgesellschaft.

---

[40] Umfassend hierzu: *Zech*, Information als Schutzobjekt, 2012, § 1 (S. 13-34) et pass.; *Albers* in: *Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle*, Grundlagen des Verwaltungsrechts, Bd. 2, 2008, § 22 Rn. 8; *Spieker gen. Döhmann* RW 2010, 247, 250 ff.; *Jendrian/Weinmann* DuD 2010, 108; *v. Lewinski*, Datenflut und Datenrecht – Informationsrecht als Deich, Kanal, Wasserhahn oder Rettungsring? (Karlsruher Dialog zum Informationsrecht), 2013, S. 5.
[41] *Giesen* PinG 2013, 62 ff.
[42] *Brink* PinG 2014, 15 ff.

2.2.2 Zuweisung von Information

Außerhalb des Datenschutzrechts bewegt sich die Rechtsordnung etwas vorsichtiger an die große informationsrechtliche Fragestellung heran. Das Immaterialgüterrecht – die ältere informationsrechtliche große Schwester des Datenschutzrechts – weist informationsrechtliche Positionen immer nur Schritt für Schritt zu. Mit den Stufungen von Urheberrechten, Leistungsschutzrechten, dem flankierenden wettbewerbsrechtlichen Schutz und dem kautelarjuristisch entwickelten Lizenzrecht tastet es sich in die terra incognita der Informationsgesellschaft vor.

Allerdings ist zu bedenken, dass dieses behutsame Vorgehen die Zuweisung der Datenschätze (einstweilen) offenlässt. Denn Information wird auch als Rohstoff der Informationsgesellschaft wahrgenommen.[43] Wem aber das Bergregal – das Königsrecht – beim *Information Mining* zusteht, ist bislang rechtlich offen. Analogien zum überkommenen Recht sind schnell gezogen, unterhalten aber mehr als dass sie weiterhelfen: Gelten hier die Regeln des Schatzfunds (§ 984 BGB)? Oder gilt eine Handstraußregelung[44], nach der jeder sich in Maßen bedienen kann? Oder vielleicht die liebevollen Regeln des BGB über den herrenlosen Bienenschwarm (§§ 961ff. BGB)?

2.2.3 Informationelle Asymmetrie als eigentliches Problem

Die eigentliche Frage, die wir in der Debatte über Überwachung adressieren, ist die eines informationellen Machtgefälles, einer informationellen Asymmetrie

[43] *Schoch* NVwZ 2006, 872, 872; *Sydow* NVwZ 2008, 481, 483.
[44] Vgl. die entsprechenden Regelungen im Naturschutzrecht (§ 39 Abs. 3 BNatSchG und speziell für Pilze § 2 BNatSchV).

oder von Überwachungsdruck. – „Wissen ist Macht“, wie wir seit *Francis Bacon* (1561–1626) wissen.[45]

Wer mit den Begriffen der „informationellen Asymmetrie“, des „informationellen Ungleichgewichts“ oder des „informationellen Gefälles“ arbeitet, sollte nicht verdecken, dass ein vollkommenes informationelles Gleichgewicht zum einen utopisch und zum anderen auch rechtlich gar nicht gewollt ist. Zwischen Staat und Bürger gibt es selbstverständlich ein Über-/Unterordnungsverhältnis, und auch im Verhältnis und im Vergleich zwischen Privaten gibt es in einer individuellen und pluralistischen Gesellschaft informationelle Unterschiede. Hinter diesem Bild steht eher das einer Waage, deren Schalen nicht notwendigerweise sich auf gleicher Höhe befinden, wohl aber in ihrem Auf und Ab verändert und einander angeglichen werden können.

Ich plädiere in diesem Zusammenhang dafür, nicht vom einen vertypten Machtverhältnis auszugehen, wie es das Datenschutzrecht mit der Zuschreibung der Rollen von „verantwortlicher Stelle“ und „Betroffenem“ tut. Sondern die Debatte um die die Überwachung sollte hinter diese Vertypung schauen, mit der uns das Datenschutzrecht vielleicht sogar den Blick verstellt.

[45] Wobei *Bacon* dies wohl weniger politisch-utilitaristisch als philosophisch-aufklärerisch meinte.

3 Überwachung und Machtbegrenzung

Wenn man also nicht mehr die Datenverarbeitung einer vertypt datenmächtigen „verantwortlichen Stelle“ als Anknüpfungspunkt von Regelungen wählt, sondern die datenmächtige Stellung als solche, kann das eigentliche Problem präziser erfasst werden.

Mit Blick sowohl auf den begrenzten Raum für diesen Beitrag wie auch auf den bisher noch jungen Forschungsstand sollen hier nur einige Leuchtkugeln verschossen werden, die aber jedenfalls illustrieren, in welche Richtung die rechtliche Begrenzung von Überwachung jenseits des herkömmlichen Datenschutzrechts gedacht werden kann.

3.1 Begrenzung von Datenmacht

Datenmacht und informationelle Asymmetrie gründen auf dem Zugriff auf Daten. Diese Datenmengen als solche zu beschränken (und nicht nur deren Verarbeitung wie das herkömmliche Datenschutzrecht), wäre ein wenngleich recht grober und holzschnittartiger Ansatz zur Begrenzung von Datenmacht.

3.1.1 Datenbegrenzung und Datenverringerung

Datensparsamkeit und Datenvermeidung sind Schlagworte, die es – ohne konkreten Regelungszusammenhang und Operationalisierung – auch in das BDSG geschafft haben, nämlich in den § 3a BDSG. Datenbegrenzungen können in unterschiedlicher Art und Weise in die Praxis umgesetzt werden: Über Löschungspflichten und einem „Recht auf Vergessenwerden“ hinaus kann an

die Einführung einer Steuer auf Gewinne, welche Unternehmen durch die Nutzung personenbezogener Daten generieren,[46] gedacht werden.

3.1.2 Verknüpfungsbeschränkungen

Weniger deutlich im Datenschutzrecht angelegt[47] – eigentlich nur in dem wenig beachteten § 10 BDSG – sind Verknüpfungsbeschränkungen. Außerhalb des Datenschutzrechts im engeren Sinne gibt es solche Regelungen in durchaus größerer Zahl: Genannt werden kann auf der verfassungsrechtlichen Ebene die Gewaltenteilung und Zuständigkeitsordnung überhaupt.[48] Im Sicherheitsbereich kennen wir das Trennungsgebot zwischen Polizei und Nachrichtendiensten. Auch die strafprozessrechtlichen und sicherheitsrechtlichen Richtervorbehalte usw. sind „Sand im Getriebe der Verknüpfbarkeit", die eine vollautomatisierte Überwachung und Datenverarbeitung erschweren. Zwar führen Richtervorbehalte kaum je zu einer Ablehnung einer Überwachungs- oder Ermittlungsmaßnahme. Es ist der bürokratische Aufwand für die Sicherheitsbehörden, der die eigentliche bremsende Wirkung entfaltet. Auch die strafpro-

---

[46] So auch *Lanier*, Googles Datenmacht, Wer die Daten hat, bestimmt unser Schicksal, F.A.Z. v. 24.04.2014, http://www.faz.net/aktuell/feuilleton/debatten/googles-datenmacht-wer-die-daten-hat-bestimmt-unser-schicksal-12907065.html; *Wedde*, Datensteuer kann die Sammelwut stoppen, http://www.nordbayern.de/nuernberger-nachrichten/politik/datensteuer-kann-die-sammelwut-stoppen-1.494270. – Ähnliche Modelle werden gegenwärtig im Internet- und Immaterialgüterbereich diskutiert und teilweise schon eingeführt. Vgl. etwa den Vorschlag von EU-Kommissar *Oettinger*, die Nutzung von in der EU geschaffenen Immaterialgütern mit einer Abgabe zu belegen (*Oettinger*, in HB v. 28.10.2014, S. 11), die spanische „Google-Steuer" auf die Verwendung von Textausschnitten (F.A.Z. v. 1.11.2014, S. 14) und die (dann nicht mehr umgesetzte) ungarische Bandbreitenbesteuerung (F.A.Z. v. 1.11.2014, S. 6).

[47] Das Datenschutzrecht kennt in § 28b Nr. 3 BDSG sogar eine Vorschrift, die eine ausdrückliche Pflicht zur Verknüpfung von Daten enthält, wenn dort die isolierte Verwendung von Anschriftendaten für das Scoring verboten wird.

[48] *v. Lewinski*, in: *Arndt u.a.*, Freiheit – Sicherheit – Öffentlichkeit, 2008, S. 196, 206 ff.

zessualen Verwertungsverbote und die Unschuldsvermutung können als eine Verwendungs- und Verknüpfungsbeschränkung begriffen werden.[49]

3.1.3 Beschränkung umfassender Datenverarbeitung

Über diese kontextabhängigen und damit relativen Datenmachtbeschränkungen hinaus sind auch noch gewissermaßen absolute Datenmachtbeschränkungen denkbar. Dies betrifft umfassende Datenverarbeitungssysteme. Beispielhaft genannt werden können das Verbot von Nummerierungssystemen (Personenkennziffern, Steueridentifikationsnummern) und die Beschränkung von Vorratsdatenspeicherungen, insb. in zeitlicher, inhaltlicher und modaler Hinsicht.[50] Kurioserweise würde auch das Scheitern der EU-DatSchGrVO zu einer solchen Beschränkung umfassender, weil binnenmarktweiter Datenverarbeitungen führen. Denn die Nicht-Vereinheitlichung der unterschiedlichen Regelungen in den 28 Mitgliedstaaten wäre dann eine automatische Bremse für die grenzüberschreitende Datenverarbeitung. Dies wird dadurch belegt, dass die Schaffung eines Binnenmarktes für personenbezogene Daten (bei der EG-DatSchRL) überhaupt die Kompetenzgrundlage gebildet hatte und jedenfalls die Ratio der EU-DatSchGrVO ist, auch wenn wegen Art. 16 Abs. 2 UAbs. 1 S. 1 AEUV wohl der Binnenmarktbezug nicht mehr unmittelbar bestehen muss.[51]

3.1.4 Staats- und Monopolbeschränkung

Beschränkt werden kann aber nicht nur der Datenbestand oder die datenmächtige Verarbeitung, sondern auch der datenmächtige Verarbeiter selbst.

---

[49] *v. Lewinski* (Fn. 19), S. 58 f.
[50] *v. Lewinski* (Fn. 19), S. 57 f.; zur zeitlichen Beschränkung *BVerfGE* 125, 260, 324; zu den Bemühungen der Bundesregierung bzgl. einer Beschränkung der Vorratsdatenspeicherung *Busch* ZRP 2014, 41, 42.
[51] *Kingreen,* in: *Calliess/Ruffert*, EUV-AEUV, 4. Auflage 2011, Art. 16 Rn. 5.

Mit dem ihm eigenen Gespür für Öffentlichkeitswirkung, inhaltlich aber durchaus berechtigt, hat der Bundeswirtschaftsminister[52] die Anwendung des Kartellrechts auf datenmächtige Unternehmen ins Gespräch gebracht. Statt einer Zerschlagung sollte hier aber eher mit der aus dem angelsächsischen Kartellrecht entlehnten Figur der Essential Facilities (§ 19 Abs. 2 Nr. 4 GWB) gearbeitet werden.[53]

Für den staatlichen Bereich würde die „Datenmachtbeschränkung durch Staatsbeschränkung" zunächst eine Rückbesinnung auf das Subsidiaritätsprinzip bedeuten. Statt Aufgaben immer mehr auf die übergeordnete Ebene – von der Kommune auf das Land, von dem Land auf den Bund, vom Mitgliedstaat auf die Europäische Union – zu verlagern, müssten sie wieder nach unten verlagert werden. Unabhängig von den Vor- und Nachteilen hinsichtlich von Steuerung und Output hätte es in Bezug auf die Datenmächtigkeit des Staates jedenfalls den Vorteil, dass nicht ein großer, potentiell Macht vermittelnder Datenbestand entstünde, sondern mehrere dezentrale Datenbestände. Diese Verringerung der Datenmacht des Staates wäre aber auch mit einer potentiell geringeren Effizienz der staatlichen Aufgabenerfüllung verbunden. In der Diskussion um die mangelhafte Fahndung und Verhinderung der Morde und Taten des rechtsradikalen „Nationalsozialistischen Untergrundes" (NSU) im den Jahren von 1999 bis 2011 hat sich gezeigt, dass die auf die Landesverfassungsschutzämter verteilte Datenmacht von der Öffentlichkeit nicht als Segen, sondern als Problem wahrgenommen wird.

[52] *Gabriel*, in: F.A.Z. v. 15.05.2014, S. 9. – Eine ähnliche Saite hat auch der Bundesjustizminister angeschlagen (*Maas*, in: F.A.Z. v. 28.06.2014, S. 4).
[53] *v. Lewinski* (Fn. 19), S. 62; ähnlicher Ansatz bei *Danckert/Meyer* MMR 2010, 219 ff.

3.2 Schaffen von Transparenz

Macht und damit auch Datenmacht kann weiter dadurch begrenzt werden, dass die Verarbeitung transparent gemacht wird. Aus der Frühzeit des Datenschutzrechts kennen wir noch umfassende Meldepflichten, die heute in den meisten Bereichen durch unmittelbare Auskunftspflichten funktional substituiert worden sind. Die Meldepflicht von personenbezogenen Datenpannen (siehe § 42a BDSG) ist ebenfalls eine solche Transparenzausprägung, die besonders die datenmächtigen Verarbeiter betrifft, weil es ja insoweit eine Erheblichkeitsschwelle gibt.[54]

Das von der Bundesregierung geplante IT-Sicherheitsgesetz will Meldepflichten dieser Art auch für den Bereich jenseits der personenbezogenen Datenverarbeitung einführen. Auch dort werden neben kritischen Infrastrukturen im Wesentlichen datenmächtige Unternehmen durch die Regelung adressiert.

3.3 Ertüchtigung der informationell Schwächeren und Selbstverteidigung

Eine Machtasymmetrie kann nicht nur durch eine Schwächung oder Fesselung des Stärkeren ausgeglichen werden, sondern auch durch eine Ertüchtigung der Schwächeren. Die Möglichkeit der Selbstverteidigung und des Selbstschutzes dient dann nicht nur der individuellen Interessenwahrung, sondern kann auch gesamtgesellschaftlich zu einem (annähernden) Informationsgleichgewicht führen.

Selbstschutz und Selbstverteidigung klingen auf den ersten Blick nach Verwirklichung von Eigenverantwortung. Das Recht und die Wahrung des Rechts in die eigenen Hände zu nehmen, ist dabei kein unproblematisches Konzept. Es passt

[54] Statt aller *Herbst*, in: *Auernhammer*, (Fn. 1), § 42a BDSG Rn. 19.

für den Wilden Westen, also einen Zustand eines noch nicht ausgebildeten Rechtstaats und Rechtswahrungssystems. Es ist dann die Reaktion auf ein Staatsversagen.

3.3.1 Informationelle Ertüchtigung

Datenschutzaufklärung und Datenschutzbildung sind Aufgaben, denen sich die Datenschutzbeauftragten seit langem und seit einiger Zeit auch die (Bundes-)Stiftung Datenschutz widmen. Eigentlich aber ist es die Aufgabe von Eltern und der Schule, Kenntnisse in Bezug auf informationelle Machtverhältnisse beizubringen.

3.3.2 Individueller Selbstschutz

Zu der informationellen Ertüchtigung gehören nicht nur Kenntnisse, sondern auch Fertigkeiten, sich gegen informationelle Zudringlichkeiten verwahren oder wehren zu können. Verschlüsselung und die richtige Auswahl von Internet-Diensten gehört hierzu, ebenso Verhaltensanpassungen[55] wie etwa (eigene) Datenaskese.

3.3.3 Gesellschaftlicher Selbstschutz

Die Summe individuellen Selbstschutzes ist dann der gesellschaftliche Selbstschutz in Informationssachen. Dies ist dann nicht nur die intellektuelle Ertüchtigung, für die lange der Name von *Frank Schirrmacher* (1959–2014) stand. Sondern die Datenverarbeiter können v.a. mit Hilfe der Medien einer sozialen

[55] *v. Lewinski* (Fn. 19), S. 66.

Kontrolle unterworfen werden; hierfür ist in Spiegelung der *Über*wachung der Begriff der *Unter*wachung geprägt worden.[56]

3.4 Informationsverfassungsrecht

Schließlich ist es für Juristen nicht fernliegend, das für die Informationsgesellschaft prägende Machtgefälle mittels der Kulturtechnik des Rechts einzuebnen. Über die einzelnen rechtlichen Regelungen soll hier nicht gesprochen, sondern zum Abschluss dieses Beitrags die Änderungen im Verfassungsrecht skizziert werden, die für eine Ertüchtigung des Grundgesetzes für das Informationszeitalter und gegen die Gefahren der informationsmächtigen Überwachung erforderlich wären.

3.4.1 Grundrechte

Wenn über den Anpassungsbedarf des Grundgesetzes im Informationszeitalter gesprochen wird, bezieht sich das meist nur auf den Grundrechtsteil.[57] Das Informationszeitalter erfordert aber gerade unter der Informationsmacht-Perspektive ein grundlegenderes Herangehen als nur das Einfügen eines Artikels zur Informationellen Selbstbestimmung.

3.4.2 Abschied von der klassisch-liberalen Ausrichtung des Grundgesetzes

So wäre im Grundrechtsteil konzeptionell wohl Abschied zu nehmen von der klassisch-liberalen Ausrichtung des Grundgesetzes nach dem Modell der klassisch-liberalen Verfassungen des 19. Jahrhunderts. Die grundrechtlichen Ge-

[56] Vgl. *Janssen* c't 12/2013, S. 74, 76; der Begriff geht auf *Steve Mann* zurück (vgl. *Monohan*, Surveillance And Security: Technological Politics And Power in Everyday Life, 2006, S. 158).
[57] Beispielhaft auch die umfassende Arbeit von *Schliesky* et al., Schutzpflichten und Drittwirkung im Internet, 2014.

währleistungen sehen wir überkommenerweise vornehmlich als Abwehrrechte des Individuums gegenüber dem Staat an. Schutzpflichten und Drittwirkungen gegenüber Privaten – vor allem Privaten aus anderen Jurisdiktionen – müssen dann erst herbeikonstruiert werden.

Wenn wir nun Datenmacht als ein strukturprägendes Element der Informationsgesellschaft ansähen, wäre es konsequent, die Schutzrichtung der Grundrechte auch auf datenmächtige private Akteure zu erweitern. Das würde dann aber auch die strukturelle Trennung von Staat und Gesellschaft, die dem Grundgesetz zugrundeliegt, aufweichen. Allerdings wären wirtschaftsbezogene Grundpflichten in der deutschen Verfassungslandschaft keine absolute Neuheit; schon die WRV und auch heute manche Landesverfassungen kennen diese dogmatische Kategorie.

3.4.3 Tariergewichte des informationellen Gleichgewichts

Informationelle Ungleichgewichte können auch durch institutionelle Ergänzungen verringert werden. Etablierte Einrichtungen hierfür sind die Datenschutzbeauftragten in Bund und Ländern, die in der jüngeren Zeit durch die Stiftung Datenschutz in Leipzig ergänzt worden sind.

Ein wesentliches Problem in diesem Zusammenhang ist das der „rationalen Apathie" der Betroffenen.[58] Datenmacht und Überwachung sind weniger fühlbar als andere Formen der Herrschaftsausübung, auch wirken sie oft zeitversetzt und schleichend. Hier wird gegenwärtig über Verbandsklagerechte nachgedacht.[59] Verfassungsrechtlich handelt es sich dabei um das grundsätzlichere Problem der Effektivität des Rechtsschutzes, die mit Blick auf die Gefahren der Informationsgesellschaft möglicherweise gesamthaftere Formen als den individuellen (Gerichts-)Prozess annehmen muss.

[58] *v. Lewinski* PinG 2013, 12, 13.
[59] *v. Lewinski* (Fn. 19), S. 77.

3.4.4 Informationelle Gewaltenteilung

Und schließlich wäre jenseits der individuellen Betroffenheit und der gesamtgesellschaftlichen Implikationen auch die innerstaatliche Machtbalance neu zu justieren. Denn die Datenmacht ballt sich innerhalb des Staates erfahrungsgemäß bei der Exekutive. Soweit ersichtlich, wird diese Frage im Gesetz lediglich in § 1 Nr. 2 hessDSG adressiert. Punktuelle Regelungen wie diese werden aber für die Anpassung des komplexen Zusammenspiels der Staatsgewalten nicht ausreichen.

4 Schluss

Die Entwicklung des Informationsrechts darf nicht nur aus einer Fortschreibung des Datenschutz- und Immaterialgüterrechts bestehen, sondern muss die Rechtsordnung gesamthaft in den Blick nehmen. Das Datenschutzrecht würde ohne eine konzeptionelle Überdehnung wahrscheinlich für seinen eigentlichen Aufgaben- und Anwendungsbereich an Wirksamkeit gewinnen. Jedenfalls ist Überwachung zu gefährlich und die Informationsgesellschaft zu wichtig, um sich an ein Recht (und eine Rechtsdogmatik) aus dem Lochkartenzeitalter zu binden.

Überwachung und Chilling Effects

Simon Assion[1]

Die Argumentation mit „abschreckenden Effekten“ ist eigentlich nicht Neues. Schon lange argumentieren Rechtsprechung und Literatur, dass bestimmte staatliche Maßnahmen nicht nur *einzelne* Personen in ihren Freiheitsrechten beeinträchtigen, sondern „einschüchternd“ auch auf große, undefinierbare Personengruppen wirken. Und doch ist die Lehre von den „Chilling Effects“ derzeit so aktuell wie nie. Denn wenn es um die rechtliche Beurteilung staatlicher Überwachung geht, betrifft diese Lehre eine Schlüsselstelle.

Überwachung kann dazu führen, dass Bürger von der Nutzung ihrer Grundrechte abgeschreckt werden. Die Frage, wie ein solcher Einschüchterungseffekt rechtlich zu beurteilen ist, ist bisher aber weitgehend ungeklärt. Offen ist insbesondere auch die Frage, ob es eine „rote Linie“ gibt, die der Staat bei der Auslösung von Chilling Effects nicht überschreiten darf. In Zeiten, in denen massenhafte staatliche Überwachung immer weiter um sich greift, wird diese Frage unmittelbar relevant.

Diese Arbeit wird den Begriff der „Chilling Effects“ mit rechtswissenschaftlichen Methoden aufarbeiten (dazu Abschnitt 1). In einem zweiten Schritt wendet sie die gefundenen Ergebnisse auf den Fall der staatlichen Massenüberwachung an, die Edward Snowden aufgedeckt hat (Abschnitt 2).

---

[1] Dieser Beitrag basiert auf einer Serie von Artikeln, die auf dem Weblog Telemedicus erschienen sind (http://www.telemedicus.info/categories/10-Chilling-Effects). Daneben fasst er – ohne Anspruch auf Vollständigkeit – den Vortrag des Autors auf der Telemedicus Sommerkonferenz 2014 zusammen. Der Autor dankt Frau *Judith Möller* und Frau *Susanne Krell* für ihre Mitarbeit.

1 Der Begriff der Chilling Effects

Der Begriff der „Chilling Effects" entstammt der angloamerikanischen Rechtstradition. Dort beschreibt er (etwas verkürzt definiert) Effekte staatlichen Handelns, die Bürger davon abhalten, von ihren Grundrechten Gebrauch zu machen; fast immer geht es dabei um die „Freedom of Speech", d.h. die Meinungsäußerungsfreiheit.[2] Abstrakt gesprochen handelt es um einen irgendwie *störenden, einschüchternden* Einfluss auf die Ausübung eines Freiheitsgrundrechts.

Teils inspiriert durch das angloamerikanische Recht, teils auch eigenständig, haben sich im deutschen Recht ähnliche Argumentationsmuster etabliert. Anders als in der englischen Rechtssprache fehlt aber im deutschsprachigen Rechtsraum eine einheitliche Begrifflichkeit, unter der die verschiedenen Erwähnungen sich zusammenfassen lassen. Dies macht es notwendig, zunächst einmal abstrakt eine eigene Definition dafür herauszuarbeiten, was „Chilling Effects" der Sache nach ausmacht (dazu Abschnitt 1.1). Ist auf diese Weise definiert, wonach eigentlich zu suchen ist, kann auch die Rechtsprechung der oberen Gerichte auf Erwähnungen von „Chilling Effects" ausgewertet werden (dazu Abschnitt 1.2). Aus der Spruchpraxis lassen sich dann auch erste Grundlinien der rechtlichen Beurteilung ableiten (dazu Abschnitt 1.3).

[2] Grundlegend siehe *Columbia Law Review* 1969, 808 ff., auch abrufbar unter http://www.jstor.org/stable/1121147; *Youn*, Vanderbilt Law Review Band 66, 1474, auch abrufbar unter http://www.vanderbiltlawreview.org/2013/10/the-chilling-effect-and-the-problem-of-private-action/.

1.1 Chilling Effects als Selbstschädigungs- und Masseneffekte

Chilling Effects haben bestimmte Eigenschaften, die sie von herkömmlichen Grundrechtseingriffen unterscheiden.

1.1.1 Chilling Effects als Masseneffekte

Zum einen sind Chilling Effects meist *Masseneffekte*. Anders als bei „herkömmlichen" Fällen der Eingriffswirkung staatlicher Maßnahmen geht es nicht um einen *einzelnen* Bürger, in dessen Rechte der Staat durch eine *konkrete* Maßnahme eingreift. Die Argumentation mit Chilling Effects taucht auf, wenn es im Ausgangspunkt zwar um einen einzelnen Grundrechtsträger geht,[3] aber die inkriminierte staatliche Maßnahme eine Vielzahl von Bürgern betrifft.[4] In der rechtlichen *Abwägung* stellen die Gerichte deshalb nicht nur auf den einzelnen Bürger ab; sie konzentrieren sich auf die Auswirkungen der staatlichen Maßnahme auf die *Allgemeinheit.* Deren Interessen werden in die rechtliche Bewertung einbezogen. Häufig führt erst die Betroffenheit der *Allgemeinheit* – und nicht die individuelle Betroffenheit des Beschwerdeführers – dazu, dass die staatliche Maßnahme als unverhältnismäßig verworfen wird.

[3] Dies erklärt sich aus dem prozessrechtlichen Hintergrund: Eine subjektive Beschwertheit des Klägers bzw. Beschwerdeführers ist in fast allen Verfahrensarten Sachentscheidungsvoraussetzung. Popularklagen sind nur in Einzelfällen zulässig.

[4] Vgl. *Oermann/Staben*, Der Staat 2013, 630, 647 f.; identisch ist die Überlegung auch im US-Recht, vgl. *Columbia Law Review* (Fn. 2), S. 808, 820 ff. m.w.N.

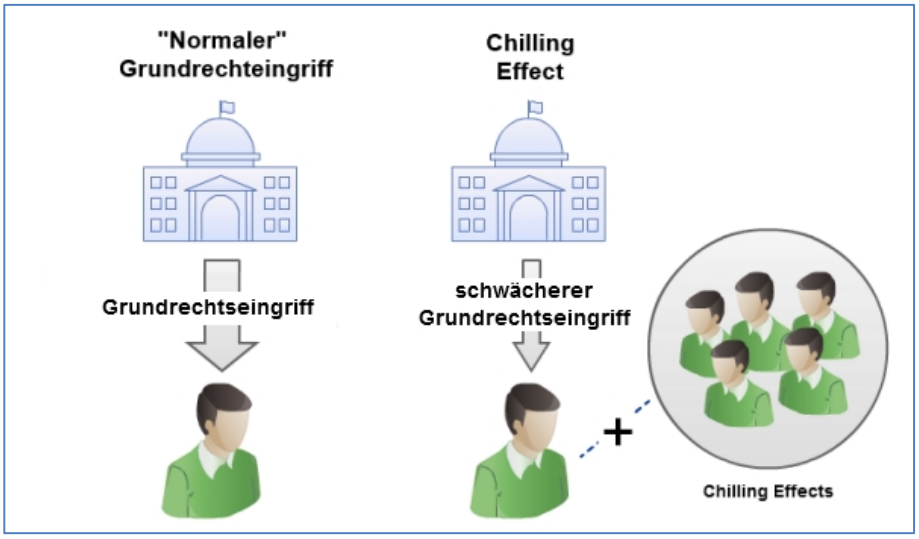


Abbildung 1: Chilling Effects als Masseneffekte

1.1.2 Chilling Effects als Selbstschädigungseffekte

Zum anderen sind Chilling Effects dadurch gekennzeichnet, dass sie nur *mittelbar*, nämlich vermittelt durch das Gefühlsleben der Betroffenen wirken. Anders als bei herkömmliche Freiheitsbeschränkungen gibt es bei Chilling Effects keine staatliche *Sanktion*, keinen unmittelbaren Zwang, der auf den Bürger wirkt. Der Bürger schränkt sich vielmehr *selbst* ein, er verzichtet *freiwillig* darauf, von seinem Recht Gebrauch zu machen.

Diese „freiwillige" Entscheidung wiederum beruht aber auf *staatlichem* Handeln, z. B. auf einem zivilrechtlich geschaffenen Haftungsrisiko oder dem Hervorrufen eines Gefühls des Überwachtwerdens.

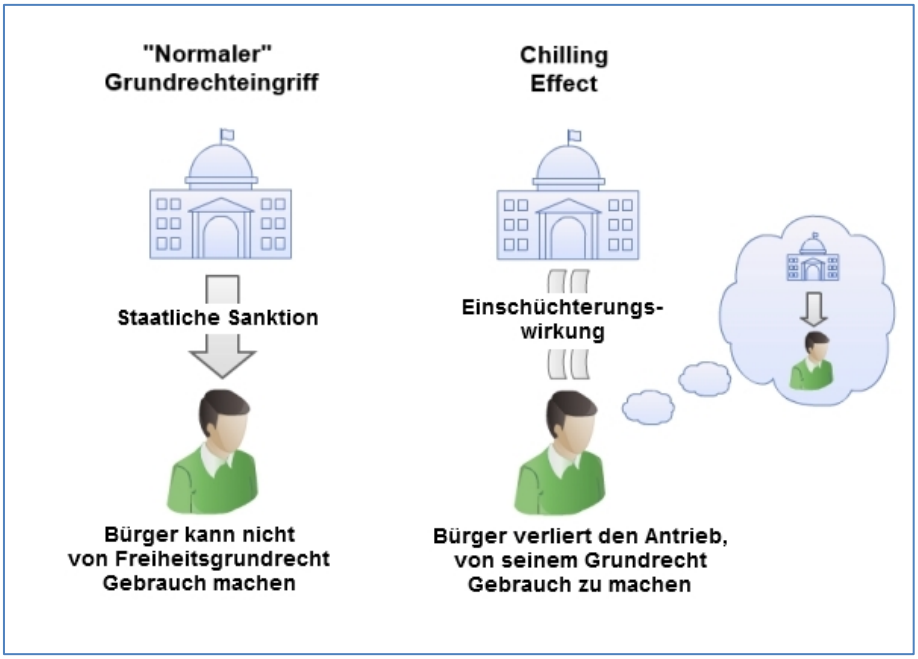


Abbildung 2: Chilling Effects als Selbstschädigungseffekte

Es ist gerade dieser etwas vertrackte Wirkmechanismus, der die Chilling Effects so schwer greifbar macht: Aus einem *greifbaren* staatlichen Handeln entsteht ein *diffuses Gefühl*[5] – und erst aus diesem Gefühl ergibt sich dann, gemeinsam mit verschiedenen anderen Einflüssen, das konkrete Handeln des Bürgers. Es gibt deshalb keine direkte Kausalbeziehung zwischen staatlichem Handeln und Freiheitsverlust, lediglich einen eher indirekten, *psychisch* vermittelten Zusammenhang.

[5] In dieser Diktion ausdrücklich *BVerfGE* 125, 260, 320 – *Vorratsdatenspeicherung*: „diffus bedrohliches Gefühl des Beobachtetseins"; *BVerfGE* 120, 378, 402 – *automatisierte Kennzeichenerfassung*: „Gefühl des Überwachwerdens"; *EuGH* v. 8.4.2014, Rs. C-293/12 und C-594/12 - *Digital Rights Ireland*, Rn. 37: „Gefühl […], dass ihr Privatleben Gegenstand einer ständigen Überwachung ist"; *BerlVerfGH* v. 11.4.2014, Az. 129/13, Rn. 49: „Gefühl des Beobachtetseins".

1.1.3 Der Staat als (Mit-)Verursacher von Chilling Effects

Generell betrachtet kann kein Zweifel daran bestehen, dass Staaten Einschüchterungseffekte als normalen Teil ihres Regierungs- und Verwaltungshandelns einsetzen.[6] So haben z. B. Angehörige der Bundeswehr eingeräumt, mit Überwachungsdrohnen in bestimmten Fällen besonders tief zu fliegen, um potentielle Kriegsgegner einzuschüchtern.[7] Auch polizeiliche Kameraüberwachung im öffentlichen Raum wird offen mit dem Motiv begründet, durch Überwachung potentielle Straftäter abzuschrecken.[8] Auch sozialwissenschaftlich ist die Existenz von Chilling Effects nachgewiesen.[9]

Die sozialwissenschaftliche Forschung zeigt aber gleichzeitig, dass die Entscheidung eines Bürgers, ein konkretes Grundrecht in einer konkreten Situation nicht zu nutzen, nicht monokausal auf einem *bestimmten staatlichen* Handeln beruht. Ein Grundrechtsträger trifft die Entscheidung zum Grundrechtsverzicht vielmehr im Ergebnis seiner *Gesamtsituation* – und diese Gesamtsituation basiert auf einer Reihe unterschiedlicher Einflussfaktoren, von denen sich nur einige dem Staat zurechnen lassen. Die Verfasserin einer sozialwissenschaftlichen Studie *Townend* nennt als maßgebliche Faktoren für Chilling Effects neben dem (staatlich verursachten) Haftungsrisiko z. B. auch

[6] In Einzelfällen wird die Einschüchterungswirkung bestimmten staatlichen Handelns durchaus bestritten. In diese Richtung z. B. die abweichende Meinung der Richter *Schluckebier* und *Eichberger*, in: *BVerfGE* 120, 260, 366 bzw. 380 f. – *Vorratsdatenspeicherung*.
[7] Siehe dazu *Assion*, Telemedicus v. 30.04.2014, http://tlmd.in/a/2703.
[8] So z. B. BVerwG v. 25.01.2012, Az. 6 C 9.11, Rn. 29 f.
[9] *Kenyon*, Internation Journal of Communication 2010, S. 440; *Townend*, Internet Policy Review v. 3.4.2014, http://policyreview.info/articles/analysis/online-chilling-effects-england-and-wales; *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, http://ssrn.com/abstract=2412564; *Sidhu,* University of Maryland Law Journal of Race, Religion, Gender and Class 2007, S. 375, 389 ff., http://digitalcommons.law.umaryland.edu/rrgc/vol7/iss2/10; vgl. auch *Oermann/Staben*, Der Staat 2013, S. 630, 644 (in Fn. 62) und S. 649 (in Fn. 76), jeweils m.w.N.

den Zugang zu Rechtsberatung bzw. das vorhandene rechtliche Wissen sowie die vorhandenen finanziellen Ressourcen.[10] Der Autor einer anderen einschlägigen Studie *Kenyon* nennt als Faktoren, die Chilling Effects im Bereich der Pressefreiheit begünstigen oder abmildern, z. B. auch die örtliche Medienkonzentration, die finanziellen Rahmenbedingungen, journalistische Traditionen im betreffenden Land und das Vorhandensein einer funktionierenden Zivilgesellschaft und politischen Opposition.[11] Dies sind Faktoren, die sich *nicht* unmittelbar dem Staat zurechnen lassen,[12] gleichwohl aber auf die Nutzung oder Nicht-Nutzung des betreffenden Grundrechtes einwirken.

Die Liste der Faktoren, die sich potentiell auf die Entscheidung eines Bürgers für oder gegen den Grundrechtsgebrauch auswirken, lässt sich beliebig fortsetzen. Ob ein Bürger im jeweiligen Fall seine Kommunikationsfreiheiten nutzt, hängt von einer Vielzahl einzelner Faktoren ab, darunter vermutlich auch dem Ausmaß des jeweils vorhandenen Fachwissens,[13] den konkret zur Verfügung stehenden Kommunikationsmöglichkeiten[14] oder simplen Rahmenfaktoren wie Alter, Geschlecht, Religionszugehörigkeit oder politischer Einstellung.

---

[10] *Townend* (Fn. 9).
[11] *Kenyon* (Fn. 9), 440, 442.
[12] Zur Vermischung von staatlichen und privaten Einflüssen *Youn* (Fn. 2).
[13] Laut dem sog. „Dunning-Kruger Effect" führt geringeres Sachwissen tendenziell zu Selbstüberschätzung und damit zur vermehrten Äußerung kaum fundierter Meinungen; siehe *Kruger/Dunning*, Journal of Personality and Social Psychology, 1999, S. 1121; allgemein auch http://de.wikipedia.org/wiki/Dunning-Kruger-Effekt.
[14] *Kenyon* (Fn. 9), 456 ff. deutet an, dass bestehende Chilling Effects teils überwunden werden können, wo Kommunikatoren die Möglichkeit haben, auf das Internet auszuweichen.

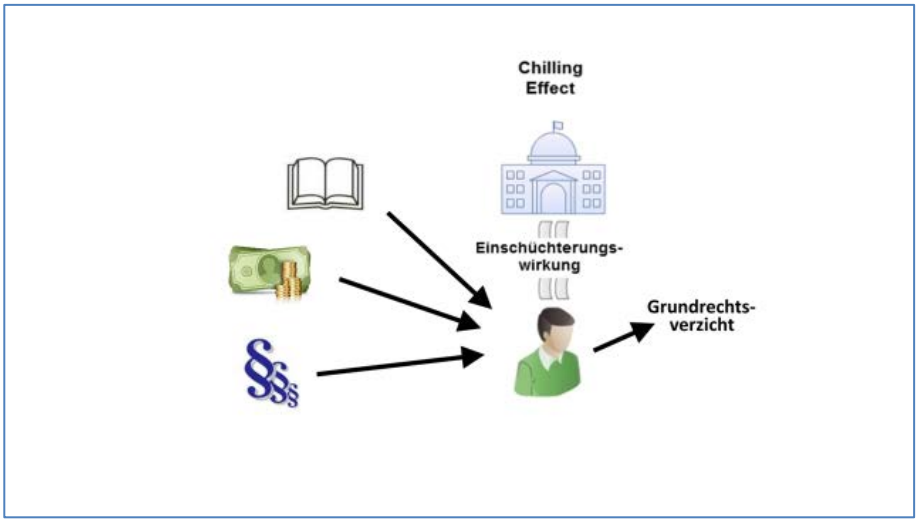


Abbildung 3: Verschiedene Auslöser von Chilling Effects

1.1.4 Arbeitsdefinition

Nach dem Vorgesagten lässt sich somit eine Arbeitdefinition des Begriffs „Chilling Effects“ ableiten:

> *„Chilling Effects entstehen, wenn staatliches Handeln – meist mit Breitenwirkung – die Bürger davon abhält, von ihren Grundrechten Gebrauch zu machen.“*

Dieses Verständnis[15] soll den weiteren Überlegungen zugrundegelegt werden.

[15] Ähnlich auch *Youn* (Fn. 2), 1474, 1481.

1.2 Chilling Effects in der Rechtsprechung

1.2.1 Überblick

Sucht man in der Rechtsprechung des BVerfG nach einer Argumentation mit den oben beschriebenen Chilling Effects,[16] finden sich entsprechende Überlegungen häufig; der Sprachgebrauch ist aber uneinheitlich. Die Gerichte sprechen von beeinträchtigenden,[17] hemmenden,[18] beengenden,[19] einschüchternden,[20] abschreckenden,[21] erschwerenden und abhaltenden[22] oder einfach nur „negativen Wirkungen auf die generelle Ausübung"[23] eines Grundrechts. Das BVerfG spricht in einigen Entscheidungen auch von Auswirkungen auf die Unbefangenheit des Grundrechtsgebrauchs[24] oder von Selbstzensur[25]. Gerade die neuere Rechtsprechung des BVerfG verwendet unmittelbar den Begriff „Einschüchterungseffekt",[26] offenbar als gezielte Anlehnung an den Begriff „Chilling Effects", der zum ständigen Vokabular des EGMR gehört.[27]

---

[16] Eine Übersicht sämtlicher ausgewerteter Rechtsprechung mit Volltextzitaten findet sich bei *Assion*, Telemedicus v. 07.05.2014, http://tlmd.in/a/2765.
[17] *BVerfGE* 73, 118, 183; *BVerfGE* 100, 313, 381.
[18] *BVerfGE* 65, 1, 43; *BVerfG* NJW 1996, 310, 310 f.; *BVerfGE* 115, 166, 188.
[19] *BVerfGE* 7, 198, 211.
[20] *BVerfGE* 43, 130, 136; *BVerfG* NJW 1996, 310; *BVerfG* v. 25. Oktober 2007, Az. 1 BvR 943/02, Rn. 38.
[21] *BVerfGE* 93, 266, 292; *BVerfGE* 99, 185, 197; *BVerfGE* 113, 29, 46; *BVerfGE* 115, 166, 188.
[22] *BVerfG* v. 25.10.2007, Az. 1 BvR 943/02, Rn. 34 ff.
[23] *BVerfGE* 43, 130, 136; *BVerfGE* 114, 339, 349.
[24] *BVerfGE* 120, 378, 402; ähnlich *BVerfGE* 100, 313, 381; *BVerfGE* 109, 279, 354 f.
[25] *BVerfGE* 73, 118, 183; ähnlich *EGMR* v. 3.12.2013, App. no. 64520/10, Rn. 73 f.
[26] *BVerfGE* 109, 279, 354 f.; *BVerfGE* 115, 166, 188; *BVerfGE* 120, 378, 402; *BVerfGE* 125, 260, 335.
[27] Soweit ersichtlich die erste Erwähnung in *EGMR* v. 27.3.1996, App. no. 17488/90 Rn. 39 - *Goodwin*; seitdem ständige Rechtsprechung, zuletzt u.a. *EGMR* v. 3.12.2013, App. no. 64520/10, Rn. 68, Rn. 73 f.

Auch der EGMR spricht allerdings nicht immer einheitlich von „Chilling Effects", sondern verwendet auch Umschreibungen, z. B. „hampering" (behindernd),[28] „deterring" (abschreckend),[29] „discouraging" (entmutigend),[30] „dissuading" (abhaltend),[31] „preventing" (vermeidend),[32] „striking"[33] (treffend) und „stifling" (erdrückend)[34].

Häufiger als das BVerfG assoziiert der EGMR die einschüchternden Effekte unmittelbar mit staatlichem Handeln. Unerwünscht ist laut dem Gerichtshof die Ausübung von Druck („pressure"),[35] die Einschüchterung („intimidation"),[36] die Drohung mit Ordnungsmaßnahmen („threat of an ex post facto review"),[37] die besitzergreifende Beeinflussung („proprietary interference in the editorial process"),[38] oder einfach nur das ins-Auge-fassen bestimmter Vorgänge („envisaged")[39]. In ständiger Rechtsprechung spricht der EGMR auch von einer Bedrohung („menace" bzw. „threat") durch Überwachung, die sich gerade auch auf die Freiheit der Kommunikation beziehe.[40] In jüngeren Entscheidungen neigt der EGMR dazu, Chilling Effects bereits ab einer recht geringen Eingriffstiefe

[28] *EGMR* v. 23.9.1994, App. no. 15890/89, Rn. 35.
[29] *EGMR* v. 27.3.1996, App. no. 17488/90, Rn. 39.
[30] *EGMR* v. 28.10.1999, App. no. 28396/95, Rn. 50; *EGMR* v. 3.5.2007, App. no. 1543/06, Rn. 67.
[31] *EGMR* v. 29.3.2001, App.no. 38432/97, Rn. 51; *EGMR* v. 2.11.2006, App. no. 13071/03, Rn. 4; *EGMR* v. 6.10.2009, App. no. 27209/03, Rn. 37; *EGMR* v. 5.7.2011, App. no. 18990/05, Rn. 68.
[32] *EGMR* v. 14.5.2013, App. no. 67810/10, Rn. 65.
[33] *EGMR* v. 06.09.1978, App. no. 5029/71, Rn. 41; *EGMR* v. 29.06.2006, App. no. 54934/00, Rn. 78, *EGMR* v. 01.07.2008, App. no. 58243/00, Rn. 56.
[34] *EGMR* v. 19.9.2013, App. no. 23160/09, Rn. 39.
[35] *EGMR* v. 13.11.2003, App. nos. 23145/93 and 25091/94, Rn. 711.
[36] *EGMR* a.a.O.
[37] *EGMR* v. 21.3.2002, App. no. 31611/96, Rn. 54.
[38] *EGMR* v. 3.12.2013, App. no. 64520/10, Rn. 73.
[39] *EGMR* v. 23.9.1994, App. no. 15890/89, Rn. 35.
[40] *EGMR* v. 06.09.1978, App. no. 5029/71, Rn. 41 - *Klass and others v. Germany*; *EGMR* v. 29.06.2006, App. no. 54934/00, Rn. 78 - *Weber and Saravia v. Germany*, *EGMR* v. 01.07.2008, App. no. 58243/00, Rn. 56 - *Liberty and others v. the United Kingdom.*

anzunehmen: Im Verfahren *Gross v. Switzerland* z. B. schon durch eine unklare Rechtslage, die für die Betroffenen zu längeren rechtlichen Auseinandersetzungen und standesrechtlichen Konsequenzen hätte führen können.[41]

Das BVerfG vermeidet eine solche unmittelbare Assoziation: Die Chilling Effects erscheinen in dessen Rechtsprechung eher als unvermeidliche *Nebenfolgen* staatlichen Handelns, z. B. von der zivilgerichtlichen Schlichtung von Streitigkeiten oder von Handlungen von Ordnungsbehörden.[42] Ein Paradigmenwechsel deutet sich allerdings in den jüngeren Entscheidungen an, die sich mit Chilling Effects aufgrund von *Überwachung* auseinandersetzen: Das BVerfG spricht darin von einem „abschreckenden Effekt fremden Geheimwissens"[43], womit der Staat gemeint ist, oder, gerade im Kontext der staatlichen Überwachung, auch von einem „bedrohlichen Gefühl des Beobachtetseins".[44] Hier erscheint der Staat als *umittelbarer* Verursacher von Chilling Effects.

Fast vollständig unbeachtet geblieben ist der Gedanke der Chilling Effects soweit ersichtlich in der Rechtsprechung des EuGH. Nur in einer Entscheidung von 2010 spricht der Gerichtshof bezüglich der Niederlassungsfreiheit von einer „abschreckenden Wirkung" auf Investoren.[45] Generell ergibt sich allerdings eine Parallele zur *Dassonville*-Formel: Nach dieser Formel beschränken nicht nur konkrete Ein- und Ausfuhrkontrollen die Warenverkehrsfreiheit,

---

[41] *EGMR* v. 14.5.2013, App. no. 67810/10.
[42] Statt vieler *BVerfGE* 54, 129, 135 f.
[43] *BVerfGE* 113, 29, 46 – *Anwaltsdaten*; *BVerfGE* 115, 166, 188 - *Online-Durchsuchung.*
[44] *BVerfGE* 125, 260, 319 - *Vorratsdatenspeicherung*; ähnlich auch *BVerfGE* a.a.O., 332 „Gefühl des unkontrollierbaren Beobachtetwerdens" und 335, „Gefühl des ständigen Überwachtwerdens"; siehe auch BerlVerfGH v. 11.4.2014, Az. 129/13, Rn. 49, „Gefühl des Beobachtetseins".
[45] *EuGH* v. 21.10.2010, Rs. C-81/09, Rn. 59 - *Idryma Typou*.

sondern auch alle „Maßnahmen gleicher Wirkung".[46] Hierzu wären sicherlich auch Abschreckungseffekte zu zählen.

Im Übrigen ist die einzige nennenswerte Andeutung der „Chilling Effects"-Argumentation durch den EuGH die jüngste Entscheidung zur *Vorratsdatenspeicherung*: Der Gerichtshof erwähnt dort, die Vorratsdatenspeicherung sei geeignet, bei den Bürgern das „Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist".[47]

1.2.2 Auswertung

Ein Überblick über die Rechtsprechung zeigt, dass der Gedanke der Chilling Effects zwar häufig, aber keineswegs immer mit der Meinungsfreiheit assoziiert wird. Versucht man eine Zuordnung zu unterschiedlichen Grund- bzw. Freiheitsrechten, zeigt sich eine breite Verteilung dieser Argumentationsfigur:[48]

- Meinungsfreiheit,[49]
- Rundfunkfreiheit,[50]

---

[46] Ständige Rechtsprechung seit *EuGH* v. 11. Juli 1974, Rs. 8/74, Rn. 2 ff. – *Dassonville*.
[47] *EuGH* v. 8.4.2014, Rs. C-293/12 und C-594/12, Rn. 37.
[48] Die Zuordnung der Gerichtsentscheidungen zu bestimmten Grundrechten ist etwas willkürlich, speziell was den *EGMR* betrifft. Denn die „Kommunikationsfreiheit" in Art. 10 EMRK ist eher allgemein formuliert und trennt nicht zwischen den einzelnen Freiheitssphären. Der *EGMR* hat dadurch die Möglichkeit, in seiner Argumentation recht frei zwischen den einzelnen Grundrechtsbestandteilen zu wechseln, ohne jeweils neu einen Schutzbereich abgrenzen zu müssen. Die Entscheidungen, die unten der Pressefreiheit zugeordnet sind, betreffen dem Wortlaut nach z. B. eher die „Freiheit des Journalismus"; der Pressefreiheit sind sie zugeordnet, weil es jeweils um Printjournalisten ging.
[49] *BVerfGE* 7, 198, 211; *BVerfGE* 43, 130, 136; *BVerfGE* 54, 129, 135 f.; *BVerfGE* 93, 266, 292; *BVerfGE* 94, 1, 9; *BVerfGE* 99, 185, 197; *BVerfGE* 114, 339, 349; *EGMR* v. 28.10.1999, App. no. 28396/95, Rn. 50; *EGMR* v. 29.3.2001, App. no. 38432/97, Rn. 51; *EGMR* v. 2.11.2006, App. no. 13071/03, Rn. 49; *EGMR* v. 19.9.2013, App. no. 23160/09, Rn. 39.
[50] *BVerfGE* 73, 118, 183; *EGMR* v. 16.10.2013, App. no. 73469/10, Rn. 80.

- Pressefreiheit,[51]
- Versammlungsfreiheit,[52]
- Wissenschaftsfreiheit,[53]
- Recht auf Privatleben,[54]
- Recht auf Entscheidung über das eigene Lebensende,[55]
- Die Funktionsfähigkeit eines Strafprozesses,[56]
- Strafverteidigung durch einen Rechtsanwalt,[57]
- Die Möglichkeit, Rechtsschutz zu suchen,[58]
- Allgemein *alle* Grundrechte bzw. die Allgemeine Handlungsfreiheit,[59]
- Niederlassungsfreiheit.[60]

---

[51] *EGMR* v. 23.9.1994, App. no. 15890/89, Rn. 35; *EGMR* v. 27.3.1996, Ap. no. 17488/90, Rn. 39 - Goodwin v. United Kingdom; *EGMR* v. 6.10.2009, App. no. 27209/03, Rn. 37 - Kulis and Rozycki v. Poland; *EGMR* v. 5.7.2011, App. no. 18990/05, Rn. 68 und 82; *EGMR* v. 3.12.2013, App. no. 64520/10, Rn. 73 f.

[52] *BVerfGE* 65, 1, 43; *BVerfGE* 122, 342, 358 f., 365 und 369; *BVerfG*, Beschluss vom 25. Oktober 2007, Az. 1 BvR 943/02, Rn. 34 ff.; *EGMR* v. 3.5.2007, App. no. 1543/06, Rn. 67.

[53] *EGMR* v. 3.12.2013, App. no. 64520/10, Rn. 68; wohl auch *EGMR* v. 19.9.2013, App. no. 23160/09, Rn. 70.

[54] *EGMR* v. 06.09.1978, App. no. 5029/71, Rn. 41; *EGMR* v. 29.06.2006, App. no. 54934/00, Rn. 78, *EGMR* v. 01.07.2008, App. no. 58243/00, Rn. 56; *EuGH* v. 8.4.2014, Rs. C-293/12 und C-594/12, Rn. 37.

[55] *EGMR* v. 14.5.2013, App. no. 67810/10.

[56] Insbesondere die unbeeinträchtigte Funktion „des staatsanwaltschaftlichen Vorgehens und der richterlichen Entscheidungsfindung", *BVerfG* NJW 1996, 310, 310 f.

[57] *EGMR* v. 21.3.2002, App. no. 31611/96, Rn. 54; *EGMR* v. 13.11.2003, App. nos. 23145/93 and 25091/94, Rn. 714; *EGMR* v. 17.7.2008, App. no. 513/05, abweichende Meinung der Richter Rozakis, Vajic und Spielmann, Rn. 8.

[58] *EGMR* v. 13.11.2003, App. nos. 23145/93 and 25091/94, Rn. 711; lesenswert zur *reformation in peius* als Chilling Effect *Columbia Law Review* (Fn. 2), 808, 837 f., auch abrufbar unter http://www.jstor.org/stable/1121147

[59] „Ausübung anderer Grundrechte" bzw. die „Freiheit des Einzelnen, aus eigener Selbstbestimmung zu planen und zu entscheiden", *BVerfGE* 65, 1, 43; *BVerfGE* 115, 166, 188; „unbefangene Wahrnehmung der Grundrechte", *BVerfGE* 125, 260, 319, bzw. „Freiheitswahrnehmung", *BVerfG* a.a.O., 332; „Handlungs- und Mitwirkungsfähigkeit" des Bürgers im „freiheitlichen demokratischen Gemeinwesen", *BVerfGE* 93, 266, 292.

Es zeigt sich somit, dass der Gedanke von der Rechtsprechung auf viele Grundrechte angewandt wird – teils sogar auf rechtlich geschütztes Verhalten, das gar nicht unmittelbar mit den Kommunikationsfreiheiten zu tun hat.[61]

Dass die Rechtsprechung die „Chilling Effects" nicht auf Kommunikationsfreiheiten beschränkt, zeigt, dass es sich weniger um eine Ausprägung eines *bestimmten* grundrechtlichen Schutzbereichs handelt, sondern eher um eine juristische Argumentationsfigur. Die Übersicht zeigt aber auch, dass die Gerichte diese Argumentationsfigur nicht *beliebig* einsetzen. Die Gerichtsentscheidungen lassen sich in zwei Fallgruppen einteilen:

- Entweder die Gerichte argumentieren mit abschreckenden Effekten, wenn sie die Unbefangenheit der Betroffenen in einem *bestimmten* Bereich als *besonders schützenswert* erachten – beispielsweise die Kommunikation zwischen Journalist und Quelle[62] oder die Aussagen von Zeugen im Strafprozess.[63] Auch die Diskussion *politischer* Belange halten die Gerichte für besonders schutzwürdig, speziell was die „Schlüsselpositionen" des politischen Diskurses angeht (Journalisten, Verlage etc.).[64] Es geht also um Verhalten, das nach Auffassung der Gerichte *besonderen* Schutz verdient.

- Oder es geht um Fälle, in denen der konkrete Eingriff nicht nur die jeweils verletzte Person betrifft, sondern als abschreckender Effekt auch die *Allgemeinheit*. Wenn ein Chilling Effect derartige *Breitenwirkung* entfaltet,

---

[60] *EuGH* v. 21.10.2010, Rs. C-81/09, Rn. 59.
[61] So auch in den USA, vgl. *Columbia Law Review* (Fn. 2), 808, 832 ff.
[62] *EGMR* v. 27.3.1996, App. no. 17488/90, Rn. 39 – *Goodwin*.
[63] *BVerfG* NJW 1996, 310, 310 f.
[64] Statt vieler *EGMR* v. 23.9.1994, App. no. 15890/89, Rn. 35; *EGMR* v. 27.3.1996, Ap. no. 17488/90, Rn. 39; *EGMR* v. 2.11.2006, App. no. 13071/03, Rn. 49; zur Rspr. des *BVerfG* siehe Fn. 133.

dass er das Funktionieren der gesellschaftlichen, demokratischen Prozesse einschränkt, wird dies von den Gerichten ebenfalls stärker gewichtet.[65]

Das BVerfG betont in diesem Zusammenhang, dass die Beinträchtigung durch Chilling Effects den „Kern" der grundrechtlich geschützten Persönlichkeitssphäre betreffen kann,[66] an anderer Stelle spricht es von einem Eingriff in die „Substanz" eines Grundrechts.[67] Der EGMR argumentiert im Grundsatz ähnlich.[68]

Die Gerichtsentscheidungen, die Bezug auf staatlich organisierte *Massenüberwachung* nehmen, lassen sich beiden Fallgruppen gleichzeitig zuordnen: Einerseits betrifft Überwachung nicht nur einzelne Personen, sondern die Gesellschaft als *Gesamtheit*. Andererseits heben die Gerichte hervor, dass die Bürger gerade auch bei den Aktivitäten eingeschüchtert werden, die für die Demokratie besonders wichtig sind (Meinungsbildung zu Themen von Allgemeininteresse, Wahlen etc.).[69] Die Gesellschaft wird dadurch in der Möglichkeit zur Selbstreflektion und Selbsterneuerung eingeschränkt.[70]

Die Entscheidungen, die sich mit Chilling Effects durch *Überwachung* beschäftigen, beziehen sich insoweit auch nicht auf *konkrete* Grundrechte; an deren

---

[65] Siehe v.a. *BVerfGE* 94, 1, 9; *BVerfGE* 99, 185, 197; *BVerfGE* 100, 313, 381; *BVerfGE* 109, 279, 354 f.
[66] *BVerfGE* 43, 130, 136; *BVerfGE* 54, 129, 135 f.
[67] *BVerfGE* 43, 130, 136; *BVerfGE* 114, 339, 349.
[68] Dass Einschränkungen der Meinungsfreiheit nicht dem Wohl der Allgemeinheit zuwiderlaufen dürfen, ergibt sich beim *EGMR* (anders als beim *BVerfG*) allerdings schon unmittelbar aus dem Gesetzestext: Schon nach dem Wortlaut des Art. 10 Abs. 2 EMRK sind Eingriffe in die Kommunikationsfreiheit nur zulässig, soweit sie „in einer demokratischen Gesellschaft notwendig" sind.
[69] *BVerfGE* 65, 1, 43 – *Volkszählungsurteil*; *BVerfGE* 113, 29, 46 – *Anwaltsdaten; BVerfGE* 115, 166, 188 – *Online-Durchsuchung; BVerfGE* 122, 342, 369 – *Bayerisches Versammlungsgesetz*.
[70] Dazu noch ausführlich in Abschnitt 2.2.1.

Stelle tritt die Erwähnung allgemein der „Freiheit der Kommunikation"[71] bzw. der „Wahrnehmung der Grundrechte in vielen Bereichen".[72]

Indem die Gerichte in den Entscheidungen zur Überwachung anerkennen, dass einschüchternde Effekte auch *gesamtgesellschaftliche* Wirkung entfalten können, lösen sie sich ein Stück weit von ihrer anderweitigen Rechtsprechung, die eher auf die Einschüchterung bestimmter Personengruppen abgestellt hatte (Journalisten etc.). Gleichzeitig ist den Überwachungs-Entscheidungen aber auch anzumerken, dass die Gerichte die abschreckenden Effekte insoweit nicht so stark gewichten wie an anderer Stelle: Wenn „Otto Normalverbraucher" sich aufgrund von Überwachung etwas *unwohl* fühlt, ist das eben nicht vergleichbar mit einem Journalisten, der wegen eines konkreten Haftungsrisikos die „Schere im Kopf" spürt und sich nicht traut, eine bestimmte Information zu veröffentlichen.

1.2.3 Was ergibt sich daraus für den NSA-Skandal?

Nach dem oben Gesagten lässt sich festhalten, dass „Chilling Effects" eine Rechtsfigur sind, die sowohl in der Rechtsprechung des BVerfG als auch des EGMR anerkannt ist und bei beiden Gerichten eine lange Tradition hat. Auch wenn die Begrifflichkeiten nicht einheitlich sind, ist doch eindeutig die Überzeugung der Gerichte erkennbar, den Grundrechten nicht nur subjektivrechtlichen Schutz zuzugestehen, sondern auch einen objektivrechtlichen Schutzgehalt, der auch einen Schutz der *Gesellschaft* gegen Einschüchterungseffekte umfasst. Die Gerichte sehen die Einschüchterungseffekte als ein Übel, das

[71] *EGMR* v. 6.9.1978, App. no. 5029/71, Rn. 41; *EGMR* v. 29.6.2006, App. no. 54934/00, Rn. 78, *EGMR* v. 1.7.2008, App. no. 58243/00, Rn. 56.
[72] *BVerfGE* 125, 260, 319 - *Vorratsdatenspeicherung*; ähnlich *BVerfG* a.a.O., 332: „Freiheitswahrnehmung".

es möglichst zu vermeiden gilt[73] und stellen diese Überlegung in ihre rechtliche Bewertung ein – meist als Teil des Abwägungsprozesses.

Ebenfalls ist festzuhalten, dass das BVerfG, der EGMR und der EuGH auch die staatliche *Überwachung* als Auslöser von Chilling Effects behandeln. Die bisherige Rechtsprechung der Gerichte behandelte allerdings immer *konkrete* Überwachungsmaßnahmen, z. B. die zeitlich begrenzte und gesetzlich eingehegte Speicherung bestimmter Telekommunikationsdaten („Vorratsdatenspeicherung"). Die Massenüberwachung, die Edward Snowden aufgedeckt hat, geht demgegenüber viel weiter.[74] Der richtige Prüfungsmaßstab muss insofern – neben individuellen Grundrechtseingriffen – auch der Effekt sein, der von der Massenüberwachung auf die *Gesamtgesellschaft* ausgeht.

In diesem Zusammenhang hat das BVerfG in seiner Entscheidung zur *Vorratsdatenspeicherung* richtigerweise auch bereits festgehalten, dass eine Gesetzgebung, „die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte [...] von vornherein mit der Verfassung unvereinbar" wäre; „die Freiheitswahrnehmung der Bürger" darf „nicht total erfasst und registriert werden".[75] Dies ist

[73] Zur Trennung zwischen „positivem" und „negativem" Chilling noch unten, Abschnitt 1.3.1.
[74] Siehe zur rechtlichen Bewertung u.a. *Hoffmann-Riem*, Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014; *Bäcker*, Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes – Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014; *Papier*, Gutachtliche Stellungnahme – Beweisbeschluss SV-2 des ersten Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode; alle abrufbar unter https://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848.
[75] *BVerfGE* 125, 260, 323.

der Bewertungsmaßstab, an dem sich auch die Geheimdienst-Massenüberwachung messen lassen muss.[76]

1.3 Dogmatische Einordnung von Chilling Effects

Die Argumentation mit Chilling Effects wird in der Rechtsprechung *häufig* eingesetzt, erscheint aber auch relativ *beliebig*. Selten wird klar, warum das Argument an einer bestimmten Stelle der Rechtsprüfung erscheint und welches Gewicht das entscheidende Gericht ihm zumisst. Auch in der Literatur fehlt es bisher fast vollständig an einer dogmatischen Aufarbeitung dieser Rechts- bzw. Argumentationsfigur. Zu Recht wurde daher die Argumentation mit Einschüchterungseffekten als „argumentativer Joker" kritisiert.[77]

Im Folgenden soll deshalb versucht werden, die Chilling Effects rechtsdogmatisch etwas greifbarer zu machen. Diese Untersuchung kann hierbei nur der Auftakt für weitere Forschung sein: Trotz der Häufigkeit und Relevanz dieser Argumentationsfigur ist sie rechtswissenschaftlich bisher kaum aufgearbeitet.[78]

Die folgende Erörterung greift drei Einzelfragen heraus. *Zuerst* soll geklärt werden, ob „Chilling Effects" per se als negativ zu bewerten sind, oder ob es auch „positives chilling" gibt (dazu Abschnitt 1.3.1). In einem *zweiten* Schritt soll herausgearbeitet werden, wofür der Staat bei Chilling Effects genau verantwortlich ist – mit anderen Worten, welches Handeln genau Anknüpfungspunkt der rechtlichen Prüfung ist (dazu Abschnitt 1.3.2). Daran anknüpfend

[76] „Überwachungsgesamtrechnung", vgl. *Roßnagel* NJW 2010, 1238, 1420; *Roggenkamp*, PinG 2014, 196, 199.
[77] *Rath*, KJ Beiheft 1/2009, 65, 70.
[78] Abgesehen von *Rath*, KJ Beiheft 1/2009, 65, 70 findet sich die soweit einzig bekannte vertiefte Auseinandersetzung mit dem Thema bei *Oermann/Staben* Der Staat 2013, 630.

lässt sich dann in einem *dritten* Schritt auch die Frage beantworten, ob Chilling Effects per se als Grundrechtseingriffe zu behandeln sind (dazu Abschnitt 1.3.3).

1.3.1 Positives und negatives „Chilling“

Die Argumentation mit Einschüchterungseffekten ist in der Vergangenheit scharfer Kritik ausgesetzt gewesen. So kommentiert Ladeur eine Entscheidung des BVerfG:

> *„Der Beschluss […] ordnet sich in eine Tendenz ein, das Grundrecht der Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1, Abs. 2 GG in einer stark individualisierten Betrachtungsweise zu einem Recht auf expressive Selbstdarstellung eigener Befindlichkeiten zu machen, der gegenüber der Öffentlichkeitsbezug der Kommunikation immer mehr zurücktritt (vgl. auch BVerfG ZUM 2013, 797). Dies entspricht auch einem in den USA vorherrschenden Verständnis, für das der Kampf gegen die Erzeugung von »chilling effects« als Folge der Sanktion von Meinungsäußerungen jede Frage nach den Schranken der Meinungsfreiheit oder gar nach deren Bedeutung für die öffentliche Meinung (Ladeur, AfP 2010, 224) zurücktreten lässt. Die Vermutungsregel hat ihren guten Sinn gehabt, solange es noch einen festen Bestand an Konventionen über die Abgrenzung von Richtigem und Falschem, von Sagbarem und des Unsagbaren gab. Inzwischen ist das Pendel längst in die andere Richtung ausgeschlagen: die Öffentlichkeit wird überschwemmt mit früher unsäglichen, maß- und haltlosen Äußerungen, die jede Unterscheidungsfähigkeit vermissen lassen. Vielfach werden komplexe Sachverhalte durch scharfe Personalisierung vereinfacht und lösen gerade dadurch in umgekehrter Richtung, bei den Adressaten der Kritik, den »chilling effect« aus, der bei den Meinungsaktivisten längst nicht mehr eintreten kann.“*

Der Kritik von *Ladeur* ist insofern zuzustimmen, als dass die Argumentation mit Chilling Effects aufgrund ihrer Unschärfe zum Missbrauch verführt. *Ladeur* hat außerdem Recht, wenn er kritisiert, dass die Argumentation mit Chilling Effects auch zu einer Überdehnung des jeweiligen Grundrechtes führen kann. Wenn nämlich jede staatliche „Einmischung" in die Frage des Grundrechtsgebrauchs automatisch als unerwünscht bewertet wird, verliert der Staat die Möglichkeit, in den Grundrechtsgebrauch der Bürger steuernd einzugreifen. Genau dies ist aber eine der grundsätzlichen Aufgaben eines Rechtsstaates: Den Freiheitsgebrauch der Bürger im Verhältnis untereinander zu moderieren und in Regeln zu fassen. Der Staat darf und muss zwischen Rechtspositionen abwägen, er darf und muss dabei auch Grundrechte einschränken. Nicht *jede* Einschränkung der Meinungsfreiheit ist deshalb verfassungsrechtlich unzulässig; erst die Tatsache, dass ein Eingriff nicht zu *rechtfertigen* ist, macht ihn unzulässig. Erst die verfassungsrechtliche Prüfung als *Ganzes* ergibt die Antwort auf die Frage, ob eine bestimmte Einschränkung mit dem Maßstab des Grundgesetzes vereinbar ist.

Ein Verständnis von Chilling Effects, die *jede* Einschüchterung als per se negativ bewertet, wäre deshalb mit dem Maßstab des Grundgesetzes nicht vereinbar. Natürlich darf der Staat Bürger beim Gebrauch ihrer Meinungsfreiheit dahingehend „einschüchtern", dass sie z. B. nicht Volksverhetzung betreiben, über andere unwahre Tatsachen behaupten oder ungerechtfertigt fremde Geheimnisse offenbaren. Dass der Staat solches Handeln mit Schadensersatz- oder Straffolgen belegt, ist eine „Einschüchterung", die ihren Sinn hat.

Es ist demnach in die Überlegung mit einzubeziehen, dass es auch „positives" Chilling geben kann.[79] Nicht jede staatliche Einschüchterung ist als negativ einzustufen. Zwischen „positivem" und „negativem" Chilling ist zu unterscheiden.

[79] *Lehofer*, e-comm v. 18.7.2011, http://blog.lehofer.at/2011/07/chilling-me-softly-wird-der-news-of.html.

Um zwischen „positivem“ und „negativem“ Chilling abzugrenzen, bietet sich eine Parallelüberlegung zur herkömmlichen Eingriffsdogmatik an. Diese gestaltet sich wie folgt:

- Immer wenn der Staat in Grundrecht *eingreift,* ist sein Handeln rechtfertigungsbedürftig. Mit anderen Worten: Nur, wenn (und soweit) der Staat sich auf die Grundrechtsschranken oder konkurrierendes Verfassungsrecht berufen kann, ist sein Handeln auch mit der Verfassung vereinbar. Auch wenn eine Rechtfertigung grundsätzlich besteht, muss der Staat sich aber an die *Schranken-Schranken* halten, insbesondere an das Verhältnismäßigkeitsgebot.
- Analog lassen sich auch die *Chilling Effects* einordnen: Demnach gilt für jedes hoheitliche Handeln, das Bürger vom Gebrauch eines Grundrechts *abschreckt*, die *Vermutung*, dass dieses Handeln „negativ“ zu bewerten ist.[80] Bewegt sich die Einschüchterung aber im Rahmen der Grundrechtschranken oder schützt sie konkurrierendes Verfassungsrecht, kann es sich ausnahmsweise auch um „positives Chilling“ handeln.[81] Wie bei der herkömmlichen Eingriffsdogmatik ist aber auch hier die Korrekturschranke des *Verhältnismäßigkeitsprinzips* einzubeziehen: Das heißt, selbst „positives Chilling“ wäre verfassungsrechtlich als negativ zu bewerten, *soweit* es eine Einschüchterung auslöst, die über den verfassungsrechtlich legitimen Effekt *hinausgeht*.[82]

Bei den durch Geheimdienstüberwachung ausgelösten Einschüchterungseffekten ist die Überlegung, es könnte sich um „positives Chilling“ handeln, eher

[80] Zu der Frage, wann Chilling Effects als Grundrechtseingriffe zu behandeln sind, sogleich in Abschnitt 1.3.3.
[81] Ähnlich *Columbia Law Review* (Fn. 2), 808, 814.
[82] Beispiel: Die Videoüberwachung einer Demonstration schreckt die Demonstranten von Straftaten ab und dient insofern einem von Art. 8 Abs. 1 GG anerkannten legitimem Zweck. Soweit sie aber von der Teilnahme der Versammlung *selbst* abschreckt, wäre sie als „negativ“ zu bewerten.

fernliegend. Dies schon deshalb, weil die Einschüchterung gar nicht das *Ziel* der Geheimdienste ist, sondern eher als unerwünschte (gleichwohl in Kauf genommene) Nebenfolge der Informationssammlung auftritt.

Anders mag das mit Überwachung in *Einzelfällen* sein:[83] So wird z. B. argumentiert, dass offene Kameraüberwachung eine einschüchternde Wirkung haben kann, die Bürger von Straftaten abhält.[84] Je nach Einzelfall ließen sich solche Maßnahmen auch nach „positives Chilling" einordnen.[85]

Die von den Geheimdiensten betriebene Massenüberwachung betrifft aber *alle* Lebensbereiche. Sie schüchtert nicht nur bei verfassungsrechtlich unerwünschtem Verhalten ein. Ganz im Gegenteil führt Massenüberwachung zu einem *Rückgang* an verfassungsrechtlich erwünschtem Verhalten.[86] Es handelt sich demnach um „negatives" Chilling.

1.3.2 Konkrete Verantwortlichkeit des Staates

In Rechtsverfahren, in denen die Zulässigkeit von Chilling Effects beurteilt werden soll, geht es regelmäßig um *staatliches* Handeln. Die Grundrechte binden die Hoheitsgewalt, nicht jedoch unmittelbar private Grundrechtsträger. Eine Abschreckungwirkung, die von *Privatpersonen* ausgeht, wird von der Abwehrfunktion der Grundrechte nicht erfasst.

---

[83] Überwachung entzieht den betroffenen die „informationelle Selbstbestimmung", nimmt ihnen also die Möglichkeit, ihr Verhalten in unterschiedlichen Lebenssphären informationell voneinander abzugrenzen. Die Folge ist ein faktischer Zwang zur Integrität, d.h. das eigene Verhalten in unterschiedlichen Rollenmustern anzugleichen. Die ambivalenten Folgen von Transparenzpflichten, denen hier nicht weiter nachgegangen wird, sind aufgearbeitet z. B. in *Jansen* et al. (Hrsg.), Transparenz – Multidisziplinäre Durchsichten durch Phänomene und Theorien des Undurchsichtigen, 2010.
[84] So z. B. BVerwG v. 25.01.2012, Az. 6 C 9.11, Rn. 29 f.
[85] *Oermann/Staben* Der Staat 2013, S. 630, 647 äußern sich allerdings zu Recht *grundsätzlich* kritisch zu Überwachung als Teil der Gefahrenabwehr.
[86] Ausführlich dazu noch in Abschnitt 2.2.1.

Diese Differenzierung wird relevant, wenn es um den rechtlichen Prüfungsmaßstab geht, der auf Chilling Effects angewendet wird. Denn oben in Abschnitt 1.1.3 ist bereits herausgearbeitet worden, dass Chilling Effects nie auf eine einzelne Ursache zurückzuführen sind. Sie entstehen als Ergebnis einer *eigenen Entscheidung* der jeweils betroffenen Bürger. Diese wiederum entscheiden sich nicht monokausal aufgrund einer einzelnen Ursache für oder gegen den Grundrechtsgebrauch, sondern beeinflusst durch eine *Rahmensituation*, die ihrerseits auf verschiedenen Einflussfaktoren beruht. Zu diesen Einflussfaktoren zählen *hoheitlich* bestimmte Determinanten genauso wie das Verhalten anderer *Privat*personen.

Es wäre insofern zu kurz gegriffen, jedes Auftreten von Chilling Effects einseitig dem Staat zuzurechnen und diesem die Pflicht aufzuerlegen, Einschüchterungseffekte generell zu beseitigen. Es überschneiden sich – auch im rechtlichen Sinne – die Verantwortlichkeitssphären der Hoheitsmacht, der betroffenen Bürger und der anderen Grundrechtsträger.[87] Insofern ist zu differenzieren:

- Die Grundrechte in ihrer *abwehrrechtlichen* Dimension gelten nur unmittelbar zwischen Bürger und Staat. Der Staat ist also in erster Linie nur verantwortlich für sein *eigenes* Handeln, nicht für andere (private) Einflussfaktoren der Chilling Effects, z. B. für den Zugang des einzelnen Grundrechtsträgers zu bestimmten Ressourcen, z. B. zu Rechtsberatung.[88] Insofern lässt sich festhalten, dass der Staat ersteinmal nur verpflichtet ist, seine *eigene* Einflussnahme auf die „Rahmensituation" der Bürger grundrechtskonform zu gestalten.
- Eine staatliche Pflicht zur Abwehr von Chilling Effects, die von *Dritten* ausgehen, wäre allenfalls mit aus Grundrechten abgeleiteten *Schutzpflich-*

[87] Siehe zu parallelen Überlegungen im US-Recht *Youn* (Fn. 2).
[88] Siehe dazu oben, Abschnitt 1.1.3.

ten begründen.[89] Eine Pflicht zum *schützenden* Eingreifen des Staates ergibt sich aber erst, wenn das sog. Untermaßverbot verletzt wird.[90] Diese Grenze ist jedoch erst bei starken Grundrechtsbeeinträchtigungen unterschritten;[91] sie verpflichtet den Staat nicht dazu, grundrechtsschützend in *jede* private Lebenssphäre einzudringen.[92]

Einschüchterungen durch Dritte muss der Staat also nur abstellen, soweit ihm dies durch eine rechtliche *Schutzpflicht* abverlangt wird. Dies wäre lediglich im Ausnahmefall anzunehmen, z. B. wenn ein Dritter die Bürger vom Grundrechtsgebrauch so stark abschreckt, dass diese Grundrechte in ihrem Kernbereich betroffen sind.

1.3.2.1 Keine unmittelbare Verantwortlichkeit für „Selbstschädigungen"

Nicht nur zwischen der Verantwortlichkeit von Staat und Dritten ist abzugrenzen, sondern auch zwischen der Verantwortlichkeit des Staates und der des betroffenen Grundrechtsträgers selbst.

Denn grundsätzlich setzt die oben gefundene Definition von Chilling Effects voraus, dass die Bürger (mehr oder weniger) *freiwillig* auf ihr Grundrecht verzichten.[93] Der Staat greift im Fall von Chilling Effects also nicht zwingend, d.h. ver- oder gebietend in die Freiheitssphäre des Bürgers ein. Er beeinflusst vielmehr lediglich die *Rahmensituation* des Bürgers dahingehend, dass dieser sich *selbst* entscheidet, ein Grundrecht nicht zu nutzen.[94]

---

[89] Zu Schutzpflichten und anderen Wirkungsdimensionen von Grundrechten im „digitalen Raum" *Hoffmann/Schulz/Borchers* MMR 2014, 89, 91 ff.
[90] *BVerfGE* 88, 203, 254 ff. – *Schwangerschaftsabbruch II*; *Schlink/Pieroth*, Grundrechte Staatsrecht 2., 29. Aufl. 2013, Rn. 110 ff.; 308 ff.,
[91] Hier ist im Einzelnen vieles umstritten; vgl. nur *Klein* JuS 2006, 960.
[92] *Michael* JuS 2001, 148, 151.
[93] Siehe dazu in Abschnitt 1.1.4.
[94] *Oermann/Staben* Der Staat 2013, 630, 641.

Rechtlich gesehen führt die Einordnung von Chilling Effects als „Selbstschädigungseffekten" zu einer grundsätzlichen Frage: Unterbricht die eigenverantwortliche, „freiwillige" Selbstschädigung des Bürgers den Zurechnungszusammenhang zum Staat? Oder muss der Staat eine Selbstschädigung der Bürger verhindern – selbst wenn diese sich selbst beschränken *wollen*?

Zugespitzt formuliert: Ist Zensur dasselbe wie Selbstzensur?[95]

Die Antwort ergibt sich letztlich aus dem freiheitlichen Prinzip der Grundrechte:[96] Wenn ein Bürger beschließt, seine Meinungsfreiheit *nicht* zu nutzen, hat er auch in *dieser* Entscheidung grundrechtlichen Schutz. Die Grundrechte schützen auch den „negativen" Freiheitsgebrauch, also z. B. das Recht, eine bestimmte Meinung *nicht* zu äußern.[97] Der Staat kann die Bürger deshalb nicht dazu *zwingen*, sich nicht einschüchtern zu lassen und ihre Grundrechte trotz der Einwirkung von Chilling Effects dennoch zu nutzen.[98]

Wenn die Bürger es demnach selbst in der Hand haben, Meinungen (nicht) zu äußern, dann kann man ein solches Verhalten dem Staat nicht unmittelbar zum Vorwurf machen.[99] Denn sein Einfluss ist begrenzt.[100] Und wo der Staat keinen Einfluss hat, ist er auch nicht verantwortlich: Hier weist das Recht dem Bürger eine Eigenverantwortung zu.

---

[95] In diese Richtung *Schulz,* in: Paschke/Berlit/Meyer, Hamburger Kommentar Gesamtes Medienrecht, 2. Aufl. 2012, 5. Abschn. Rn. 79.
[96] Einprägend formuliert bereits in *BVerfGE* 5, 85, 204 f. – *KPD-Verbot*.
[97] Statt vieler *Schemmer*, in: BeckOK GG, Stand 01.09.2014, Art. 5 Rn. 16.
[98] Konkret limitiert hier das Übermaßverbot (ein *Zwang* des Bürgers zum Grundrechtsgebrauch wäre unverhältnismäßig) die Schutzpflicht des Staates, der Chilling Effects verhindern soll. Siehe zu dieser Konstellation *J. Isensee*, in: *Isensee/Kirchhoff*, Hdb. des Staatsrechts, Band IX, 3. Aufl. 2011, § 191 Rn. 316 ff.
[99] Wohl a.A. unter dem Hinweis, auch Einwirkungen auf das „forum internum" beträfen einen grundrechtlich geschützten Bereich *Oermann/Staben* Der Staat 2013, 630, 641.
[100] Zu Grundrechten als „negativen Kompetenznormen" *Schlink/Pieroth* (Fn. 90), Rn. 91.

Damit lässt sich festhalten: Für den Chilling *Effect*, d.h. das selbstschädigende Verhalten der Bürger, ist der Staat nicht verantwortlich.

1.3.2.2 Verantwortlichkeit des Staates für eigenes Handeln

Der Staat ist nach dem Vorgesagten aber nicht von *jeder* Verantwortung freigesprochen. Denn natürlich muss der Staat zumindest für das Handeln verantwortlich sein, das er durch seine Organe selbst vornimmt, das ihm direkt zurechenbar ist. Es ist insofern nicht die *Selbstschädigung* der Bürger, die zum grundrechtlichen Anknüpfungspunkt wird – es ist die externe staatliche *Einwirkung* auf die Rahmensituation, in der sich der Bürger befindet.

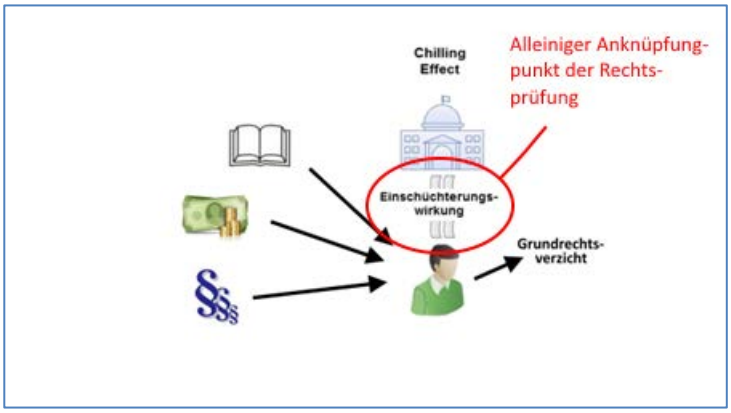


Abbildung 4: Konkrete Verantwortlichkeit des Staates

Somit gilt: Wirkt eine staatliche Einwirkung auf die Bürger derart „abschreckend", dass sie für den Bürger eine spürbare Einschränkung beim Grundrechtsgebrauch bedeutet, muss sich der Staat sich für diese *Einwirkung* rechtlich verantworten.[101] Insbesondere gilt das, wenn der Staat *gezielt* Abschreckungseffekte hervorruft.[102]

[101] Ähnlich *Oermann/Staben* Der Staat 2013, 630, 642 f.
[102] OVG Lüneburg NJW 2006, 391, 392.

1.3.3 Sind Chilling Effects Grundrechtseingriffe?

Unter Rückgriff auf das oben Ausgeführte lässt sich auch die Frage beantworten, ob Chilling Effects als solche Grundrechtseingriffe sein können, d.h. ob sich die staatliche Einwirkung an den Grundrechtsschranken messen lassen muss.[103]

In diesem Zusammenhang ist zunächst darauf hinzuweisen, dass die Frage, ob ein Grundrechtseingriff vorliegt, von der h.M. nicht nur nach der *Intention* des staatlichen Handelns, sondern auch nach seinem (grundrechtseinschränkenden) *Effekt* beantwortet wird.[104] Rechtsprechung und Lehre haben sich zu Recht schon lange vom sog. „klassischen Eingriffsbegriff" gelöst, der als Voraussetzung eines Eingriffs ein *finales*, *imperatives*, *rechtsförmiges* und mit *Sanktionswirkung* versehenes staatliches Handeln voraussetzte. Es gilt die Lehre vom „modernen" Eingriffsbegriff, bei dem auch staatliches Handeln ohne unmittelbare Zwangswirkung als Eingriff gewertet werden kann.[105] Dies gilt z. B. auch für Informationshandeln[106] (sog. „mittelbar-faktische Eingriffe"[107]). Notwendig ist dann aber, dass das staatliche Handeln den Grundrechtsgebrauch „erschwert"[108] und dabei eine gewisse *Erheblichkeitsschwelle* überschreitet.[109]

---

[103] Hier nicht weiter thematisiert wird die mit diesem Gedanken verbundene Anforderung der *Beschwerdebefugnis*. Da staatliche Maßnahmen, die keine Grundrechtseingriffe sind, wohl auch keine subjektive Beschwertheit auslösen, können Einzelpersonen sie schlecht vor Gericht angreifen. Hier sprechen gute Gründe für eine Rücknahme dieser Anforderungen, um auch solche staatlichen Maßnahmen prüfen zu können, die ihre verfassungsrechtliche Schädlichkeit nicht bei einzelnen Personen erreichen, sondern als *Masseneffekte* (oben Abschnitt 1.1.1). So verfährt zumindest die US-Rechtstradition, vgl. *Columbia Law Review* (Fn. 2), 808, 820 ff. m.w.N.
[104] *Oermann/Staben* Der Staat 2013, 630, 637.
[105] *Oermann/Staben* Der Staat 2013, 630, 637.
[106] *BVerwGE* 87, 37, 41 ff. – *Glykolwein; BVerfGE* 105, 279, 299 ff. – *Osho.*
[107] *Kaiser* JuS 2009, 313, 313.
[108] *Kaiser* JuS 2009, 313, 313.
[109] *Murswiek* NVwZ 2003, 1, 2; *Oermann/Staben* Der Staat 2013, 630, 637.

Es kommt also darauf an, ob der Staat durch eigenes Verhalten eine Einschüchterungswirkung hervorruft, die den Grundrechtsgebrauch derart erschwert, dass die Einschüchterung eine gewisse Spürbarkeitsschwelle überschreitet. Damit ist nicht ausgeschlossen, dass das Bestehen von Chilling Effects auch zur Annahme eines Grundrechtseingriffs führt. Es kommt aber darauf an, (1.) ob die konkrete Einschüchterungsmaßnahme die Verhaltensänderung *bezweckt* und (2.) wie intensiv die Einschüchterung *wirkt*.[110]

Auch Überwachung kann eine solche Einschüchterungswirkung verursachen und deshalb als „mittelbar-faktischer" Eingriff zu werten sein.[111] Ab welchem Punkt die Überwachungs-Einwirkung die Erheblichkeitsschwelle überschreitet und damit zum Grundrechtseingriff wird, ist aber im Einzelfall zu entscheiden und eine Wertungsfrage.[112] Grundsätzlich lässt sich sagen: Sobald ein Einschüchterungseffekt für den einzelnen *direkt erkennbar* wird, sobald er also einen direkt auf ihn und seinen Grundrechtsgebrauch gerichteten staatlichen Einfluss *spüren* kann, verursacht einschüchternde Überwachung auch insoweit[113] einen Grundrechtseingriff.[114]

Wichtig ist, dass die Frage nach der Erheblichkeit bzw. Spürbarkeit des staatlichen Handelns für jedes Grundrecht *gesondert* zu betrachten ist. Denn ein staatliches Handeln, das im Bereich des einen Grundrechts nur einschüchternd

---

[110] *Murswiek* NVwZ 2003, 1, 2.
[111] Lesenswert *Oermann/Staben* Der Staat 2013, 634, 637 ff.
[112] *Oermann/Staben* Der Staat 2013, 630, 655 nennen drei Kriterien: Das Vorliegen eines „Abschreckungszusammenhangs", eine massen- und dauerhafte Wirkung und die individuelle Betroffenheit des Beschwerdeführers.
[113] Auf einen „Eingriff durch Einschüchterung" in z. B. die Meinungsfreiheit kommt es bei Überwachung nicht an, da darüberhinaus *unmittelbar* vor Überwachung schützende Grundrechte betroffen sind; dazu sogleich unten.
[114] Bejaht für die polizeiliche Durchsuchung aller Teilnehmer einer Versammlung vom *BVerfG*, Kammerbeschluss vom 12.5.2010, 1 BvR 2636/04 Rn. 15; ebenfalls bejaht für die Videoüberwachung einer Demonstration bei BerlVerfGH v. 11.4.2014, Az. 129/13, Rn. 49; differenzierend OVG Münster v. 23.11.2010, Az. 5 A 2288/09, Rn. 4 f.

wirkt, kann im Bereich eines anderen Grundrechts ein klarer und eindeutiger Grundrechtseingriff sein. Genau so ist es im Regelfall bei der Überwachung: Staatliche Überwachung mag auf Ebene der Meinungsfreiheit nur als „Chilling Effect" zu werten sein, der die Erheblichkeitsschwelle für sich gesehen noch nicht überschreitet. Unabhängig davon liegen Grundrechtseingriffe aber vor, wenn die Überwachung z. B. private Telekommunikation betrifft (Art. 10 GG), in Wohnungen eindringt (Art. 13 GG), die Vertraulichkeit und Integrität informationstechnischer Systeme beeinträchtigt (IT-Grundrecht, Art. 1 Abs. 1, Art. 2 Abs. 1 GG) oder der Staat personenbezogene Daten erhebt, speichert oder deren Zweck ändert (Grundrecht auf informationelle Selbstbestimmung, Art. 1 Abs. 1, Art. 2 Abs. 1 GG).[115]

Letztlich liegt hierin der Grund, warum die Frage, ob Chilling Effects Grundrechtseingriffe sind, dogmatisch bisher kaum aufgearbeitet ist: Es kommt darauf meist nicht an. „Chilling Effects" sind eine Argumentationsfigur, die meist *begleitend* zu anderen Rechtsprüfungen eingesetzt wird; die Frage nach ihrer Qualität als Grundrechtseingriff stellt sich dann gar nicht.

Dennoch sind Chilling Effects – unabhängig von ihrer Einordnung als Grundrechtseingriffe – überall dort in eine rechtliche Prüfung einzubeziehen, wo die Interessen der Allgemeinheit für die Rechtsbewertung relevant sind. Insbesondere gilt dies nach der Lehre von der objektiv-rechtlichen Wirkung der Grundrechte dort, wo sich ein Rechtstatbestand für solche allgemeinen Erwägungen öffnet, also insbesondere bei unbestimmte Rechtsbegriffen und Abwägungen zwischen verschiedenen Rechtsgütern. Regelmäßig betrifft das die Verhältnismäßigkeitsprüfung.[116] Hier taucht die Argumentation mit den „Chilling Effects" in der Praxis auch am häufigsten auf.

---

[115] *Hoffmann-Riem* (Fn. 74), S. 5 ff.
[116] So auch im US-Recht, vgl. *Columbia Law Review* (Fn. 2), 808, 822.

2 Chilling Effects und Überwachung

Im dritten Abschnitt dieser Erörterung soll es darum gehen, die in den ersten beiden Abschnitten gefundenen Erkenntnisse auf den Fall der NSA-Überwachung anzuwenden.

2.1 Ausmaß und Umfang der Überwachung

Die von Edward Snowden in die Wege geleiteten Enthüllungen betreffen die massenhafte Informationserhebung durch die NSA und die mit ihr verbündeten Geheimdienste; darunter maßgeblich auch das britische GCHQ und der deutsche Bundesnachrichtendienst. Das gesamte Ausmaß dieser Überwachung liegt nicht offen. Edward Snowden und andere Whistleblower haben nur Teile offenlegen können; von diesen Offenlegungen haben die Medien nur Teile publiziert. Ob die Aussagen von Snowden stimmen, lässt sich zwar einer Plausibilitätskontrolle unterziehen, aber nur sehr beschränkt auf Richtigkeit prüfen. Denn die Zusammenhänge, um die es geht, sind Gegenstand staatlichen Geheimnisschutzes; dies erschwert die Beweisführung in Rechtsverfahren.[117]

Ein Überblick über den *Gesamtumfang* der Überwachung, der auch für die hiesige Einschätzung von Chilling Effects relevant ist, liegt allerdings vor.[118] Die Enthüllungen von Snowden haben gezeigt, dass es gegenüber bestimmten Geheimdiensten – und damit gegenüber bestimmten Staaten – faktisch keine Privatsphäre mehr gibt.[119] Zusammengefasst ist es der Ansatz der NSA und der

[117] Exemplarisch: BVerwG vom 28.05.2014, Az. 6 A 1.13, Rn. 20 ff. – *Härting*; für eine Reduktion der Beweispflichten in der Rspr. des *EGMR* siehe oben Fn. 33.
[118] Zusammenfassend *Greenwald*, No Place To Hide – Edward Snowden, the NSA and the Surveillance State, 2014, S. 90 ff.; *Rosenbach/Stark*, Der NSA-Komplex – Edward Snowden und der Weg in die totale Überwachung, 2014, S. 120 ff.
[119] *Rosenbach/Stark* (Fn. 118), S. 272 ff.

mit ihr verbundenen Geheimdienste, zunächst *alle* verfügbaren Daten zu erheben, dann möglichst *alles* davon zu speichern, zu filtern, auszuwerten und mit verbündeten Diensten zu teilen.[120] Oder wie Snowden es gegenüber den Mitgliedern eines Untersuchungsausschusses des EU-Parlamentes ausgedrückt hat: *„I am telling you that without getting out of my chair, I could have read the private communications of any member of this committee, as well as any ordinary citizen. I swear under penalty of perjury that this is true."*[121]

Das Vorgehen der Geheimdienste lässt sich als *arbeitsteilig* beschreiben: Daten, die vom einen Geheimdienst erhoben wurden, werden von anderen ausgewertet und mit weiteren Daten zusammengeführt; wieder andere greifen auf die gesammelten Erkenntnisse zu und setzen sie in Form konkreter Operationen um.[122] Die Dienste tauschen dabei nicht nur die jeweiligen *Ergebnisse* ihrer Geheimdienstarbeit untereinander aus, sondern auch die Daten als Rohmaterial oder in nur oberflächlich gefilterter Form. Getauscht wird auch die zur Auswertung notwendige Software.[123]

Auch deutsche Behörden, insbesondere der BND und das ihm vorgesetzte Bundeskanzleramt, haben Massenüberwachungsmaßnahmen angeordnet und sich Medienberichten zufolge an massenhaftem Datenaustausch mit der NSA und anderen Geheimdiensten beteiligt.[124] Eine besonders wichtige Rolle spielt auch der GCHQ, der zum Vereinigten Königreich gehört – und somit zu einem Staat der EU und des Europarats.

---

[120] *Greenwald* (Fn. 118), S. S. 97; *Rosenbach/Stark* (Fn. 118), S. 123.
[121] Eingabe von *Edward Snowden* an den Justizausschuss des EU-Parlamentes, abrufbar unter http://www.blamethegame.respect-my-privacy.eu/Snowden_answers.pdf.
[122] *Rosenbach/Stark* (Fn. 118), S. 240 ff.
[123] *Rosenbach/Stark* (Fn. 118), S. 244 ff.
[124] *Mascolo/Leyendecker/Goetz*, Süddeutsche.de v. 4.10.2014, http://sz.de/1.2157432; *Rosenbach/Stark* (Fn. 118), S. 240 ff.

Die rechtliche Grundlage für solche Kooperationen ist zweifelhaft. Einzelne Ermächtigungsgrundlagen lassen sich evtl. im BND-Gesetz oder im NATO-Truppenstatut finden. Wie weit diese reichen, ist jedoch in vieler Hinsicht diskutabel[125] – speziell auch hinsichtlich der Verfassungs- und Europarechtskonformität dieser Normen. Denn ein Gesetz, das massenhaft Chilling Effects auslöst, ist u.U. selbst mit höherrangigem Recht nicht vereinbar.

2.2 Zum rechtlichen Bewertungsmaßstab

Den Gesamtkomplex der Snowden-Enthüllungen einer rechtlichen Bewerung zuzuführen, ist nicht einfach. Hier soll ein Teilaspekt besonders beleuchtet werden: Inwieweit die durch die Massenüberwachung ausgelösten Chilling Effects sich auf die rechtliche Gesamtbewertung auswirken, speziell bei der Frage der Vereinbarkeit von Überwachungsmaßnahmen mit den Grundrechten.

2.2.1 Chilling Effects und die Kommunikationsverfassung

Wie oben bereits herausgearbeitet wurde, lässt sich insbesondere aus der EMRK, der EU-GrCh dem GG das rechtliche Gebot ableiten, dass der Staat durch sein Handeln möglichst keine Chilling Effects auslösen darf.[126] Dieser Gedanke soll nicht nur durch die oben bereits zitierte Rechtsprechung belegt werden, sondern im Folgenden auch durch eigene Überlegungen zur Schutzbedürftigkeit der *Unbefangenheit* der Grundrechtsträger in einer parlamentarischen Demokratie.

2.2.1.1 Der rechtliche Schutz des demokratischen Diskurses

Anlasslose Überwachung schüchtert nicht nur in einzelnen, abgrenzbaren Zusammenhängen ein, sondern ganz *allgemein* bei der Teilnahme an allen

[125] *Deiseroth* ZRP 2013, 194; *Bäcker* (Fn. 74), S. 3 ff.
[126] Siehe dazu insbesondere Abschnitt 1.2.3.

gesellschaftlichen Prozessen. Es geht somit nicht nur um konkrete Grundrechte, sondern auch um die Verfassungsrechtsgüter, die das *Funktionieren der Gesellschaft als solche* betreffen.[127] Allen voran ist dies das in Art. 20 Abs. 1 GG niedergelegte Demokratieprinzip.[128] Dieses ist selbst wieder vor dem Kontext der in den Grundrechten ausgelegten Wertordnung auszulegen. So ergibt sich das Bild einer komplexen „Kommunikationsverfassung",[129] die die gesellschaftliche Kommunikation in all ihren Aspekten schützt, aber bestimmte Bereiche besonders heraushebt und absichert: Die individuellen Kommunikationsgrundrechte, die Mediengrundrechte,[130] die Grundrechte für besonders wichtige Kommunikationsarten (Kunst, Wissenschaft, Forschung, Lehre), die Versammlungen, Vereine und Parteien als „Katalysatoren" der Meinungsbildung, die Glaubensgemeinschaften, Familien und Wohnungen als private Rückzugsorte vor staatlicher Einflussnahme und natürlich das Recht auf unmittelbare, freie, geheime und gleiche Wahl.[131] Diesen so verfassungsrechtlich umrahmten demokratischen Diskurs muss ein demokratischer Staat schützen.

Die Demokratie ist auf einen gut funktionierenden Kommunikationsprozess angewiesen. Nur durch Wahlen, die nach einem fairen „Meinungskampf" durchgeführt wurden, kann eine Demokratie sich legitimieren. Und nur ein offener, Minderheitsmeinungen schützender und die Vielfalt der Meinungen widerspiegelnder Kommunikationsprozess kann gewährleisten, dass eine Gesellschaft sich immer wieder neu erfindet – und zu Lösungen für die Probleme kommt, die sich ihr in einer immer komplexer werdenden Welt stellen.[132]

---

[127] *Oermann/Staben* Der Staat 2013, 630, 646.
[128] *Grzeszick*, in: *Maunz/Dürig*, GG, Stand 71. EL 2014, Art. 20 Rn. 17.
[129] *Schulz* AfP 2013, 464.
[130] *Schulz* AfP 2013, 464, 465 unter Verweis auf *BVerfGE* 20, 162, 174 f. – *Spiegel*.
[131] Vgl. auch *Scholz*, in: *Maunz/Dürig* (Fn. 128), Art. 5 Abs. 3 Rn. 13 ff.; *Schulz* AfP 2013, 464, 465 f.
[132] Siehe ausführlich auch Abschnitt 7.1.2.3 der Doktorarbeit des Verfassers, „Must Carry – Übertragungspflichten auf digitalen Plattformen", im Erscheinen.

Das BVerfG hat diesbezüglich von einem „Meinungskampf" gesprochen;[133] bereits in der *Spiegel*-Entscheidung auch von einem Prozess der „ständigen Diskussion".[134] Präziser lässt sich von einem *demokratischen Diskurs* sprechen, in dem Meinungen und politische Präferenzen untereinander konkurrieren oder sich gegenseitig ergänzen und befruchten, teils miteinander verschmelzen oder aufeinander aufbauen.[135] Letztlich mündet dieser öffentliche Diskurs in verschiedene Formen von Regierungs- und Verwaltungshandeln und demokratischer Mitbestimmung ein.[136] Je besser dieser Diskurs funktioniert – je besser also die Öffentlichkeit und die von ihr beeinflussten Entscheidungsträger in der Lage sind, zwischen richtig und falsch, zwischen zweckmäßig und unzweckmäßig, angemessen und unangemessen etc. zu unterscheiden, desto besser entwickelt sich auch das Allgemeinwohl.[137] Das rechtliche System der Kommunikationsverfassung, die auf der historischen und individuellen Erfahrung der Mütter und Väter des Grundgesetzes beruht, soll diesen demokratischen Diskurs als *solchen* schützen, es macht nicht bei einzelnen Grundrechten halt.[138] Nicht nur die einzelnen Bürger sind zu schützen, auch der Diskurs als sozialer Prozess darf durch die Hoheitsgewalt nicht „eingefroren" werden.[139]

---

[133] *BVerfGE* 7, 198, 208 ff.; *BVerfGE* 24, 278, 285; *BVerfGE* 25, 256, 264 f.; *BVerfGE* 27, 71, 79; *BVerfGE* 42, 163, 170; *BVerfGE* 43, 130, 139; *BVerfGE* 54, 129, 137 ff.; *BVerfGE* 54, 208, 217 ff.; *BVerfGE* 61, 1, 7; *BVerfGE* 62, 230, 244 f.; *BVerfGE* 66, 116, 139 f.; *BVerfGE* 70, 138, 172; *BVerfGE* 73, 206, 258; *BVerfGE* 82, 272, 282; *BVerfGE* 85, 1, 16; *BVerfGE* 124, 300, 324 f.; siehe auch *Hoffmann-Riem*, in: Benda et al., Hdb. des Verfassungsrechts, § 7 Rn. 12.
[134] *BVerfGE* 20, 162, 174 – *Spiegel.*
[135] Zum Diskursbegriff *R. Keller*, Wissenssoziologische Diskursanalyse, S. 99 ff.
[136] *Meyer*, in: *Isensee/Kirchhof*, Hdb. des Staatsrechts, Band III, 3. Aufl. 2003, § 45 Rn. 12 ff.; *BVerfGE* 119, 181, 214 ff. – *Rundfunkfinanzierungsstaatsvertrag*.
[137] *BVerfGE* 20, 162, 174 f. – *Spiegel*.
[138] *Oermann/Staben* Der Staat 2013, 630, 645 ff.; allgemein *Schmitt-Glaeser*, in: *Isensee/Kirchhof* (Rn. 136), § 38.
[139] *Oermann/Staben* Der Staat 2013, S. 630, 645.

2.2.1.2 Die besondere Bedeutung von Minderheitsmeinungen

Wenn das BVerfG auf den Topos „Meinungskampf" abstellt, ist der Begriff zwar missverständlich, hebt aber zutreffend hervor, dass der demokratische Diskurs auch von Merkmalen der *Konkurrenz* geprägt ist. Der Wettbewerb der Meinungen entscheidet über die hoheitliche und politische Steuerung der Gesellschaft. Da dieser Wettbewerb ständig läuft und sich immer wieder neu entscheidet, kann sich die Gesellschaft veränderten Verhältnissen anpassen. So entwickelt sie sich weiter.

Im demokratischen „Meinungskampf" beginnen alle neuen Meinungsströmungen als *Minderheitsmeinungen*: Lange bevor eine Meinung zur Mehrheitsmeinung werden kann, wird sie zunächst erst einmal von einer kleinen Gruppe von Personen vertreten. Dies führt in keiner Weise dazu, dass Minderheitsmeinungen rechtlich gesehen weniger legitim wären; sie sind für die Erneuerungsfähigkeit der Gesellschaft sogar *besonders* wichtig. Zwar weiß niemand, *welche* Minderheitsmeinungen sich in zwanzig Jahren durchgesetzt haben werden; ein Großteil wird verworfen und vergessen sein. Ein Teil der Auffassungen der Bevölkerung wird sich aber ändern – falls der Diskurs funktioniert, zum besseren.

Bis eine Meinung sich durchgesetzt hat, braucht sie als Minderheitsmeinung einen wirkungsvollen Schutz. Denn in einer Demokratie regiert die Mehrheit. Und ohne Minderheitenschutz hindert nichts die Mehrheit daran, ihre Auffassung nicht nur mit *kommunikativen* Mitteln zu behaupten, sondern auch mit Mitteln der staatlichen Machtausübung, z. B. mittels zweckfremder Instrumentalisierung des Strafrechtes oder anderer Gesetze, die über die Zulässigkeit von

Kommunikationsvorgängen entscheiden.[140] Genau dies würde aber die Fähigkeit der Gesellschaft zur Selbsterneuerung beeinträchtigen.[141]

Ein Beispiel: Noch vor wenigen Jahrzehnten war gelebte Homosexualität in Deutschland eine Straftat, denn die demokratische Mehrheit wollte eine Strafverfolgung Homosexueller. Heute hat dieser Wert sich gewandelt, Homosexualität gehört zum öffentlichen Leben und wird (größtenteils) anerkannt. Kaum jemand würde heute noch in Frage stellen, dass gleichgeschlechtliche Liebe sein darf und dass es gut war, dass diese Meinung sich durchgesetzt hat. Damit dies möglich war, brauchten diejenigen, die sich für „Gay Rights" einsetzten, aber den (grund-) rechtlichen Schutz einer Minderheit: Das Recht, sich zu Homosexualität zu äußern, darüber zu forschen und zu publizieren, sich künstlerisch damit auseinanderzusetzen, sich zu Aktivistengruppen zusammenzutun und dafür zu demonstrieren, etc.

Weil niemand vorher weiß, *welche* Minderheitsmeinungen sich später einmal durchsetzen und mehrheitsfähig werden, brauchen *alle* Minderheitsmeinungen einen geschützten Raum. Dieser Schutz schließt auch den Schutz vor Einschüchterung mit ein, wie oben bereits herausgearbeitet wurde und weiter unten noch genauer ausgeführt werden wird.

2.2.1.3 Die besondere Rolle von „Meinungsführern"

Neben der besonderen Rolle der Vertreter von Minderheitsmeinungen soll noch auf eine zweite gesellschaftliche Gruppe eingegangen werden: Die sog.

---

[140] Neben dem Strafrecht ist z. B. noch das Jugendmedienschutzrecht, das Datenschutzrecht und das Urheberrecht zu nennen.

[141] Hinzu kommt, dass die repressive Unterdrückung von Minderheitsmeinungen, denen keine faire Chance auf Durchsetzung eingeräumt wird, die Vertreter dieser Meinungen in die Illegalität drängt, was häufig zu sozialem Unfrieden bis hin zu Gewalt und Terrorismus führt. Zum „befriedenden" Effekt der Chilling Effects-Doctrine *Columbia Law Review* (Fn. 2), 808, 826.

„Meinungsführer".[142] Dies sind Personen, die nach kommunikationswissenschaftlichen Erkenntnissen für die gesellschaftliche Meinungsbildung eine besondere Rolle spielen.[143] Zu dieser Gruppe gehören Multiplikatoren wie Journalisten und Blogger, aber auch Personen mit Autorität im jeweiligen Umfeld, wie Gewerkschaftsführer, Pfarrer, Unternehmenslenker und Amtsträger.[144] Hier lassen sich auch Personen nennen, die gezielt darauf *hinarbeiten*, am Diskurs mitzuwirken, z. B. Politiker, Künstler, Wissenschaftler und Aktivisten. Diese „Opinion Leader" gehen den Dingen deutlich mehr auf den Grund, sie informieren sich tiefer und spezifischer und sie tauschen sich auch untereinander aus.[145]

Die überwiegende Mehrheit der Bevölkerung orientiert sich einerseits an Meinungsführern im direkten Umfeld, andererseits an Massenmedien, die ihrerseits wieder von Meinungsführern gesteuert und befüllt werden.[146] Auf diese Weise bildet sich ein *Diskurs im Diskurs*: Die Meinungsbildung vollzieht sich zuerst innerhalb einer kleinen, elitären Gruppe, bevor die Meinungen(en) nach und nach in die breite Masse durchsickern.

2.2.1.4 Zwischenergebnis

Die besondere Bedeutung von Minderheitsmeinungen und Meinungsführern gilt es auch bei der Rechtsanwendung zu berücksichtigen. Gerade wenn es um Chilling Effects geht, spielt diese Erkenntnis eine Rolle. Denn Meinungsführer,

---

[142] *Gladwell*, Tipping Point – Wie kleine Dinge großes bewirken können, 4. Aufl. 2002, 41 ff.
[143] Ausführlich *Dressler/Telle*, Meinungsführer in der interdisziplinären Forschung: Bestandsaufnahme und kritische Würdigung, 2009.
[144] *Dressler/Telle* (Fn. 143), S. 25 ff.
[145] Zusammenfassend *Schenk*, Medienwirkungsforschung, 3. Aufl. 2007, S. 366 ff.
[146] *Krüger*, Meinungsmacht. Der Einfluss von Eliten auf Leitmedien und Alpha-Journalisten - eine kritische Netzwerkanalyse, 2013.

insbesondere solche aus Minderheitengruppen, werden von Chilling Effects *besonders* betroffen.[147]

Die Reaktion der Gesellschaft auf eine abweichende Meinung kann brutal sein, auch in einer Demokratie; Meinungsführer wissen dies, viele haben einschlägige Erfahrungen gemacht oder sie im Umfeld miterlebt.[148] Selbst für Bundestagsabgeordnete etablierter Parteien gehören Grenzverletzungen wie z. B. Drohbriefe, Beleidigungen und Angriffe im Stil von z. B. eingeworfenen Scheiben zum Alltag. Erst Recht gilt dies für Vertreter von Minderheitsmeinungen. Dies sind Angehörige von Gruppen, die gesellschaftlich ohnehin bereits ausgegrenzt werden. Tritt nun eine *staatliche* Einflussnahme mit Einschüchterungseffekt hinzu, verstärkt dies eine ohnehin bestehende Einschüchterung noch zusätzlich.[149]

Meinungsführer in Minderheitsgruppen können – gerade in einer (durch die *Mehrheit* beherrschten) Demokratie – nicht zwangsläufig davon ausgehen, dass sie vom Staat in jeder Situation geschützt werden. Die Rahmenbedingungen, unter denen diese Personengruppe sich für oder gegen den Grundrechtsgebrauch entscheidet, sind somit tendenziell meinungsäußerungsfeindlich. Dies steht diametral dem gesellschaftlichen Bedürfnis entgegen, *gerade* die Meinungsäußerungen in den Diskurs einzuspeisen, die kontrovers sind und von der Mehrheit nicht geteilt werden. Denn nur von solchen „Minderheitsmeinungen“ kann Innovation ausgehen.

---

[147] Siehe zunächst die folgenden Ausführungen; Belege sind in Abschnitt 2.2.1.5 zitiert.

[148] Gerade auf die Snowden-Enthüllungen haben die demokratischen Staaten USA und Großbritannien mit offensichtlich unverhältnismäßigen und repressiven Methoden reagiert, darunter die erzwungene Landung (symbolische) Zerstörung von Datenträgern in den Räumlichkeiten des *Guardian*; vgl. dazu *Rosenbach/Stark* (Fn. 118), S. 16 ff.

[149] Zur Einschüchterung von Moslems *Sidhu* (Fn. 9), S. 375, 389 ff.

.

Als Zwischenergebnis lässt sich an dieser Stelle festhalten, dass Chilling Effects, um die Innovationsfähigkeit einer Gesellschaft nachhaltig zu beeinträchtigen, nicht die *gesamte Breite* der Bevölkerung erfassen müssen. Der demokratische Diskurs hat neuralgische Punkte; er kann schon durch die Einschüchterung kleiner Personengruppen geschädigt werden. Dies sind einerseits die „Opinion Leader", andererseits die Vertreter von Minderheitsmeinungen – und vor allem die *Schnittmenge* dieser beiden Gruppen, d.h. die *Meinungsführer*, die sich für *Minderheitsmeinungen* einsetzen.

Ein aktueller Beispielsfall: Es ist bekannt, dass die NSA gezielt prominente Moslems überwacht hat, und zwar auch solche, die nicht im Entferntesten im Verdacht stehen, den Terrorismus zu fördern.[150] Diese Überwachung betraf Angehörige einer Minderheit: Die politische Betätigung von Moslems steht in vielen gesellschaftlichen Sphären der westlichen Welt unter Generalverdacht, gerade wenn es sich um Moslems handelt, die ihren *Glauben* auch politisch begreifen. Gleichzeitig besteht aber *gerade* über die mit der politischen Auslegung des Islam verknüpften Fragen enormer gesellschaftlicher Diskussionsbedarf. Der demokratische Diskurs ist darauf angewiesen, sich mit diesen Fragen auseinanderzusetzen und möglichst viele Informationen, verschiedene Sichtweisen und Deutungsvarianten verarbeiten zu können. Wie soll das aber funktionieren, wenn eine der relevantesten Gruppen an diesem Diskurs nicht oder nur sehr zaghaft teilnimmt, weil sie eingeschüchtert wurde?

Diese Gefahr besteht nicht nur theoretisch: Bereits vor Bekanntwerden der Massenüberwachung waren Einschüchterungseffekte bei Moslems nachweisbar.[151] Es ist offensichtlich, dass diese Einschüchterung sich nur verschärft haben kann: Wie soll ein muslimischer Meinungsführer auf die Information reagieren, dass seine gesamte normale Kommunikation, verdachtsunabhängig

[150] *Greenwald/Hussain*, The Intercept v. 9.7.2014, https://firstlook.org/theintercept/2014/07/09/under-surveillance.
[151] *Sidhu* (Fn. 9), S. 375, 389 ff.

und außerhalb einer funktionierenden rechtlichen oder demokratischen Kontrolle gespeichert und ausgewertet wird?[152] Kann ein Meinungsführer unter diesen Umständen ausschließen, dass die Informationen nicht zweckentfremdet und/oder zum Anknüpfungspunkt staatlicher Willkürmaßnahmen werden? Gilt dies für die *gesamte* Dauer der – potentiell unbegrenzten –Speicherung dieser Informationen? Kaum ein Meinungsführer wird diese Fragen sämtlich mit „Nein" beantworten können.

2.2.1.5 Chilling Effects durch Überwachung

Inwieweit Massenüberwachung unter den aktuellen Rahmenbedingungen Chilling Effects auslöst, ist schwer einzuschätzen; es gibt aber bereits erste Forschungsergebnisse.

In einer Studie, die im August 2014 veröffentlicht wurde, zeigen *Marthews* und *Tucker*, dass Nutzer von Google nach Bekanntwerden der NSA-Massenüberwachung signifikant[153] seltener nach Suchworten suchten, die sie als „gefährlich"[154] empfanden.[155]

Die Studie von *Marthews* und *Tucker* fragte nach einer Änderung des Verhaltens *aller* Bürger; sie maß nicht die Einschüchterungswirkung auf bestimmte Personengruppen (z. B. die sog. „Opinion Leader"). Zu letzterer Frage liegen seit

---

[152] Die NSA hat mehrfach darauf verwiesen, Daten in anderen Staaten "legal" erhoben zu haben und meint, damit, dass die Datensammlungen vom FISA-Court genehmigt wurden, d.h. einem ausschließlich US-Interessen verpflichteten Geheimgericht (*Rosenbach/Stark* (Fn. 118), S. 237 ff. und 274 ff.). Aus Sicht eines Nicht-US-Bürgers, der sich außerhalb der USA bewegt, fehlt es damit an jeder externen Aufsicht und Kontrolle der NSA, die ihn schützen würde.
[153] Innerhalb der USA ca. 5 %, vgl. *Marthews/Tucker* (Fn. 9), S. 15.
[154] *Marthews/Tucker* (Fn. 9), S. 10 f. verwendeten eine Liste von Begriffen, die ihrerseits zuvor darauf gefiltert wurden, ob sie für die Betreffenden Probleme verursachen oder peinlich werden könnten („we asked participants to rate this term by how likely it is that it would `get them into trouble' or `embarrass' them with their family, their close friends, or with the US government").
[155] *Marthews/Tucker* (Fn. 9), S. 13 ff.

Oktober 2013 die Ergebnisse einer internen Umfrage von *PEN America* vor. PEN ist eine Organisation von Schriftstellern, Journalisten und Übersetzern, die sich gezielt der Förderung des politischen Diskurses verschrieben hat; zu ihren Mitgliedern gehören einige der bekanntesten Schriftsteller der USA. Die Mitglieder von PEN America sind insofern ein anschauliches Beispiel für eine Gruppe von Personen, die einerseits als *Meinungsführer*, andererseits als Vertreter (oder Vermittler) von *Minderheitsmeinungen* für den demokratischen Diskurs besonders wichtig sind.[156]

Die für die hiesige Untersuchung wichtigsten Ergebnisse der Umfrage unter den PEN-Mitgliedern sind:

- 24 % der antwortenden PEN-Mitglieder haben am Telefon oder per E-Mail eine Kommunikation über bestimmte Themen vermieden.[157]
- 16 % haben es vermieden, über ein bestimmtes Thema zu schreiben – weitere 11 % haben es ernsthaft in Betracht gezogen.[158]
- 16 % haben es vermieden, zu einem bestimmten kontroversen Thema online zu recherchieren, weitere 12 % haben dies ernsthaft in Betracht gezogen.[159]
- Themen, die von PEN-Mitgliedern als „gefährlich" empfunden wurden: Der Nahe Osten, der Snowden-Skandal, Occupy, der „War on Drugs".[160]

Die Umfrage von PEN zeigt deutlich, dass die Einschüchterungswirkung der Geheimdienst-Überwachung unter den PEN-Mitgliedern deutlich stärker wirkt als in der allgemeinen Bevölkerung. Sie zeigt auch, dass die Einschüchterungs-

---

156 Siehe die Selbstdarstellung unter http://www.pen.org/about.
157 *PEN America*, Chilling Effects – NSA Surveillance Drives U.S. Writers to Self-Censor, 2013, abrufbar unter http://www.pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf, S. 6.
158 *PEN America* (Fn. 157), S. 6.
159 *PEN America* (Fn. 157), S. 6.
160 *PEN America* (Fn. 157), S. 6.

wirkung *gerade* die Bereiche erfasst, wo der demokratische Diskurs ein unbefangenes, nicht-eingeschüchtertes Verhalten von (Minderheits-) Meinungsführern am meisten braucht.

Niemand wird jemals sagen können, wie viele Zeitungs- und Blogartikel, Romane und Sachbücher, Theaterstücke, Filme, Radiofeatures und Interviews zu kontroversen Themen nicht entstehen werden, weil deren potentielle Schöpfer zu sehr eingeschüchtert waren. Aber nach den Ergebnissen der Umfrage von PEN America ist klar: Die Einschüchterungswirkung der Geheimdienst-Massenüberwachung ist real vorhanden, und sie schädigt spürbar den demokratischen Diskurs.

Dass Überwachung einen öffentlichen Diskurs lähmen kann und welche Folgen dies hat, ist auch *historisch* belegt: In allen diktatorischen Staaten der Neuzeit gehörte Massenüberwachung zu den Repressionsmitteln. Insbesondere das Beispiel der *DDR* zeigt, wie der öffentliche Diskurs darunter leidet, wenn „Meinungsführer" eingeschüchtert werden: Der Umgang der DDR mit abweichenden Meinungen war offen repressiv, auch in Bereichen ohne direkten Bezug zum Sozialismus, z. B. der Umweltbewegung.[161] Ein Großteil der Bevölkerung arrangierte sich mit den bestehenden Machtverhältnissen, solange die allgemeinen Lebensverhältnisse ausreichend gut waren. Nur eine kleine Gruppe von Bürgern, die sich gerne kontrovers mit gesellschaftlichen Themen befasst hätte, litt unter staatlichen Willkür- und Einschüchterungsmaßnahmen, darunter auch der Massenüberwachung. Genau diese Gruppe wäre es aber gewesen, die sich für eine Modernisierung der Gesellschaft eingesetzt hätte. Nicht nur für parlamentarische Demokratie, sondern z. B. auch für Umweltschutz, eine neue Kulturpolitik oder wirtschaftliche Innovation. Weil der Diskurs nicht funktionierte, stagnierten die Verhältnisse. Die Folge waren die Verarmung der öffentlichen Debatte und Kultur, die Zerstörung der Umwelt, ökonomischer Verfall –

[161] *Neubert*, Geschichte der Opposition in der DDR 1949-1989, 2. Aufl. 1998, S. 445.

und letztlich eine allgemeine Eintrübung der öffentlichen Stimmung, die (gemeinsam mit anderen Ursachen) zur friedlichen Revolution kulminierte.

Auch dieses Beispiel zeigt: Die rechtliche und politische Eingrenzung von Überwachung vor Überwachung schützt zunächst vor allem eine Minderheit, ist aber letztlich im Interesse der allgemeinen Mehrheit.

2.2.2 Internationaler Grundrechteschutz

Schon die schiere Menge der Überwachungsmaßnahmen, die enthüllt wurden, macht den rechtlichen Zugriff schwierig. Und auch die Beweislage ist nicht einfach, da Geheimdienste naturgemäß im Geheimen arbeiten. Ein weiteres Problem liegt in der *internationalen Dimension* der Überwachung, denn es geht um kooperatives, *grenzüberschreitendes* Handeln der Geheimdienste. In juristischer Hinsicht führt dies zu Fragen des öffentlichen Kollisionsrechts;[162] speziell zu der Frage, welche nationalen Grundrechte für welche Geheimdienste eigentlich gelten – und welchen Rechtsschutz *internationale* Grundrechtevereinbarungen vermitteln.

Dass die nationalen Grundrechte einen „territorialen" Anwendungsbereich haben, d.h. die Tätigkeit von Geheimdiensten im Ausland nicht erfassen, ist eine beliebte These der Sicherheitsbehörden.[163] Darüber lässt sich allerdings streiten.[164]

Eine umfassende Auseinandersetzung mit diesem Argument würde hier den Rahmen sprengen. Grob lassen sich aber die folgenden Grundlinien skizzieren:

---

[162] Zum Begriff *Ruffert*, in: *Möllers* et al., (Hrsg.), Internationales Verwaltungsrecht, 2007, 398 ff.; vgl. auch *Ewer/Thienel* NJW 2014, 30, 31.
[163] Siehe *Bäcker* (Fn. 74), S. 18.
[164] Siehe u.a. *Hoffmann-Riem* (Fn. 74), S. 10 ff.; *Bäcker* (Fn. 74), S. 18 ff.; *Ewer/Thienel* NJW 2014, 30.

- Die NSA ist eine Behörde der USA. Als solche ist sie gem. dem *Grundsatz der Staatenimmunität*[165] dem deutschen Recht nicht unterworfen (Art. 25 GG, § 20 Abs. 2 GVG).[166] Als US-Behörde beachtet die NSA nur US-Recht, insbesondere die *US-Constitution* und deren Amendments. Der Schutz der US-Constitution für Ausländer ist sehr begrenzt.[167]
- Daneben gilt für *alle* beteiligten Geheimdienste, inkl. der US-Behörden, der *internationale Pakt für Menschen- und Bürgerrechte* (IPbR).[168] Art. 17 IPbR schützt vor Eingriffen in die „Korrespondenz", was sich als Schutz des Brief- und Telekommunikationsgeheimnisses interpretieren lässt.[169] Art. 19 IPbR schützt die Meinungsfreiheit. Individuellen Rechtsschutz gibt es nach dem IPbR aber nicht.[170]
- Anders als die NSA unterfallen zumindest der britische Geheimdienst GCHQ und andere europäische Geheimdienste der *Europäischen Menschenrechtskonvention*, insb. Art. 8 und 10 EMRK, und dem *EU-Recht,* insb. Art. 7, 8 und 11 der EU-Grundrechtecharta und Art. 16 AEUV.[171] Auch hier ist die rechtliche Bewertung aber komplex, da die Anwendbarkeit der jeweiligen Grundrechte sowohl sachlich (Einschlägigkeit) als auch territorial in Zweifel gezogen werden kann.[172]
- Aus hiesiger Sicht wohl am wichtigsten: Die deutsche Hoheitsgewalt unterfällt voll der Anwendbarkeit des *Grundgesetzes*. Dies gilt auch für Eingriffe

---

[165] Grundsätzlich zum Grundsatz der Staatenimmunität *Roeder* JuS 2005, 215; *Geiger* NJW 1987, 1124; zur Nichtanwendung dieses Grundsatzes auf die Strafverfolgung ausländischer Spionage aber *BGH* NJW 1995, 1811.

[166] *Ewer/Thienel* NJW 2014, 30, 31 verweisen, jedenfalls was ausländische Überwachung auf deutschem Boden angeht, auf das völkerrechtliche Nichteinmischungsgebot.

[167] Siehe *Cole*, Georgetown Law Faculty Publications and Other Works, Paper 297, http://scholarship.law.georgetown.edu/facpub/297.

[168] *Kotzur* ZRP 2013, 216, 217.

[169] Wie weit dieser Schutz effektiv reicht, ist aber zweifelhaft, vgl. *Kotzur* ZRP 2013, 216, 217; *Ewer/Thienel* NJW 2014, 30, 32.

[170] *Ehlers/Becker*, Europäische Rechte und Grundfreiheiten, S. 27.

[171] *Ewer/Thienel* NJW 2014, 30, 32 ff.

[172] Eine *EMRK*-Verletzung bejahen aber *Ewer/Thienel* NJW 2014, 30, 32 ff.

im Ausland, denn die Grundrechte des GG binden die deutsche Hoheitsgewalt weltweit; soweit es um Menschenrechte geht, auch gegenüber Nicht-Deutschen.[173] Grundrechtsverpflichtet sind insbesondere der Bundesnachrichtendienst und die deutsche Bundesregierung, soweit sie Massenüberwachung fördern oder ermöglichen.[174]

Je nachdem, welche Institution jeweils gehandelt hat, gelten also unterschiedliche Grundrechtekataloge, die unterschiedlich intensive Schutzwirkung haben. Festhalten lässt sich, dass alle betroffenen Grundrechtekataloge grundsätzlich auch die Meinungsfreiheit und die Privatsphäre schützen, wenn auch nicht mit identischem Wortlaut und mit identischem Schutzumfang. Der Schutz vor staatlicher Überwachung und die Eindämmung von „Chilling Effects" lässt sich jedenfalls im Ausgangspunkt somit *allen* Grundrechtekatalogen zuordnen. Welcher Grundrechtekatalog jeweils greift, ist aber eine Frage des konkreten Sachverhalts und der rechtlichen Bewertung im Einzelfall.

2.2.3 Zurechenbarkeit von Grundrechtseingriffen

Gerade ausgehend vom deutschen Verfassungsrecht stellt sich die Frage, wie Handlungen von *ausländischen* Geheimdiensten zu beurteilen sind. Denn bei den meisten aufgedeckten Überwachungsmaßnahmen geht es nicht um die Handlung einer einzelnen staatlichen Organisation, sondern um das kooperative, arbeitsteilige Handeln mehrerer Geheimdienste unterschiedlicher Staaten.[175] Und auch die Überwachung selbst hat häufig grenzüberschreitende Dimension: Die staatliche *Überwachungshandlung* erfolgt auf dem eigenen Staatsgebiet, ihr *Effekt* auf einem anderen. Für nationale Grundrechtekataloge,

---

[173] Vgl. insb. *BVerfGE* 100, 313, 363 ff. – *Telekommunikationsüberwachung I*; *Papier* (Fn. 74), S. 7 ff.
[174] Zu „geheimen Verwaltungsvereinbarungen" und der auch anderweitig unzureichenden Rechtslage *Deiseroth*, ZRP 2013, 194.
[175] *Rosenbach/Stark* (Fn. 118), S. 240 ff.

deren Geltungsbereich sich häufig territorial bestimmt, ist ein solcher Zusammenhang nur schwer zu fassen.

Die Frage, inwieweit bei internationalen Kooperationen von Hoheitsträgern deren Grundrechtsverletzungen wechselseitig *zugerechnet* werden können, scheint in Rechtsprechung und Lehre bisher kaum erörtert worden zu sein.[176] Dies spricht dafür, Anleihen in anderen Rechtsgebieten zu nehmen, wo Zurechnungsfragen häufiger relevant werden. Greift man auf zivilrechtliche oder strafrechtliche Dogmatik[177] zurück, sind der deutschen Hoheitsgewalt zumindest die Grundrechtseingriffe voll zurechenbar, von denen deutsche Hoheitsträger *wussten* und auf deren Ablauf sie einen steuernden *Einfluss nehmen* konnten, z. B. aufgrund von arbeitsteiligem Vorgehen bei der Umsetzung eines gemeinsamen „Tatplans" (Mittäterschaft).[178]

Vor diesem Maßstab betrachtet sind die grundrechtsunterworfenen deutschen Geheimdienste für Grundrechtseingriffe der NSA oder des GCHQ zumindest insoweit mitverantwortlich, als sie diese trotz Kenntnis geduldet und unterstützt haben.[179]

Selbst wenn man eine Zurechnung von Grundrechtsverletzungen zwischen kooperativ handelnden Geheimdiensten ablehnt, lässt sich auf den *Schutzgedanken* der Grundrechte verweisen.[180] Im Zeitalter der Globalisierung, insbesondere von multilateralen und supranationalen Sicherheitskooperationen

---

[176] Siehe dazu *Bäcker* (Fn. 74), S. 20 f. m.w.N.; *Papier* (Fn. 74), S. 6 unter Verweis auf *BVerfGE* 66, 39, 62.
[177] § 25 StGB, § 278 BGB, § 830 BGB.
[178] So wohl auch *Papier* (Fn 74), S. 7 f.; *Ewer/Thienel* NJW 2014, 30, 35; zurückhaltender *Bäcker*, Erhebung, Bevorratung und Übermittlung von Telekommunikations-daten durch die Nachrichtendienste des Bundes – Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014, 19 f.
[179] *Bäcker* (Fn. 74), S. 21; *Papier* (Fn. 74), S. 7 ff.; *Ewer/Thienel* NJW 2014, 30, 35.
[180] Siehe dazu bereits in Abschnitt 1.2.3; außerdem *Hoffmann-Riem* (Fn. 74), S. 15 ff.

spielt es für den Bürger letztlich keine Rolle, welcher Staat und welche staatliche Organisation die für ihn die maßgeblichen negativen Folgen bewirken.[181] Oder anders gesagt: Ein Bürger, der sich in einer globalen Welt und einem globalen Kommunikationsraum bewegt, hat aus Privatsphäreverletzungen durch *britische* oder *US*-Geheimdienste ähnlich starke Nachteile wie aus solchen der *deutschen* Behörden. Wenn ihn der deutsche Staat vor Übergriffen nicht schützt, spielt es für den Bürger letztlich keine Rolle, wo seine Daten gespeichert und ausgewertet werden. Die negativen Folgen der Überwachung treffen ihn von „oben", d.h. vermittelt durch eine mit Hoheitsrechten ausgestattete Macht. Dies gilt speziell für Überwachung durch „befreundete" Geheimdienste, denn diese agieren in einem Bündnis mit deutschen Behörden und werden durch diese unterstützt.

Der deutsche Staat muss sich zumindest dann *schützend* vor die Grundrechte seiner Bürger stellen, wenn diese Beeinträchtigungen seitens Dritter ausgesetzt sind, die verfassungsrechtlich nicht mehr vertretbar sind.[182] Dies gilt speziell für den Menschenwürdekern dieser Grundrechte.[183] Ob die Überwachung durch NSA, GCHQ etc. diesen Level überschritten hat, lässt sich angesichts des Ausmaßes und der Intensität der Überwachung durchaus diskutieren.[184] Die Frage stellt sich allerdings nur theoretisch.[185] Denn unabhängig von der Frage der Verletzung von *Schutzpflichten* lassen sich ausreichend Hinweise auf *eigene* Mitwirkungen der deutschen Dienste an Grundrechtsverletzungen finden, z. B. durch die Zurverfügungstellung von Datenmaterial oder die Einräumung des

[181] In diese Richtung auch *Ladeur*, in: *Möllers* et al. (Fn. 162), S. 377 ff.
[182] Hier ist im Einzelnen vieles umstritten; vgl. nur *Klein* JuS 2006, 960; *Schlink/Pieroth* (Fn. 90), Rn. 110 ff.; 308 ff., *Michael* JuS 2001, 148, 151.
[183] *Papier* (Fn. 74), S. 12.
[184] *Papier* (Fn. 74), S. 6 ff.; *Deiseroth* ZRP 2013, 194 ff.; *Ewer/Thienel* NJW 2014, 30, 34 f.
[185] So zur Auslandsaufklärung des BND auch *Bäcker* (Fn. 74), S. 21.

Zugriffs auf die Infrastruktur von Dritten.[186] Diesbezüglich gilt zunächst eine Pflicht, diese eigenen Mitwirkungshandlungen zu *unterlassen*.

[186] Speziell zur „Lieferung" personenbezogener Daten an die NSA durch den BND *Mascolo/Leyendecker/Goetz*, Süddeutsche.de v. 4.10.2014, http://sz.de/1.2157432.

3 Rechtliche Ableitung / Ergebnis

Was lässt sich aus den vorigen Ausführungen für die rechtliche Bewertung der Massenüberwachung ableiten?

Zunächst einmal ist oben herausgearbeitet worden, dass „Chilling Effects“ als Rechts- und Argumentationsfigur sowohl in der Rechtsprechung des EGMR als auch des BVerfG etabliert sind. Die Rechtsprechung ist teils wenig systematisch, aber ein „roter Faden“ ist erkennbar: Die Gerichte sind der Auffassung, dass die Einschüchterung von Bürgern beim Grundrechtsgebrauch aus verfassungs- bzw. grundrechtlicher Sicht unerwünscht ist.

Staatlich verursachte Einschüchterung wird von den Gerichten besonders dann als negativ bewertet, wenn sie entweder ein *besonders schützenswertes Verhalten* betrifft (z. B. die Kommunikation zwischen den Beteiligten eines Gerichtsverfahrens) oder sich als *Masseneffekt* auf die breite Bevölkerung auswirkt. Für Massenüberwachung gilt beides: Einerseits betrifft sie besonders wichtiges Verhalten, nämlich die Teilnahme an der politischen Meinungsbildung und demokratischen Mitbestimmung. Andererseits betrifft dieser Chilling Effect (wenn auch mit unterschiedlicher Intensität) die *gesamte* Gesellschaft. Die Aussage, dass Massenüberwachung verfassungsrechtlich unerwünscht und ab Überschreiten eines gewissen Grades automatisch verfassungswidrig ist,[187] gehört zur ständigen Rechtsprechung des BVerfG und des EGMR.[188]

Auch wenn die gerichtliche Argumentation mit Chilling Effects in der Vergangenheit häufig recht beliebig wirkte, lassen sich Chilling Effects auch rechts*dogmatisch* greifbar machen. Zum einen lässt sich konkret benennen, wofür der

[187] „Überwachungsgesamtrechnung“, vgl. *Roßnagel* NJW 2010, 1238; *Roggenkamp* PinG 2014, 196, 199.
[188] Siehe dazu die Hinweise in Abschnitt 1.2.3.

Staat bei „Chilling Effects“ verantwortlich ist: Für sein *eigenes* Handeln, in Form der hoheitlichen *Einwirkung* auf die *Rahmensituation*, in der Bürger sich für oder gegen den Grundrechtsgebrauch entscheiden. Erfolgt das staatliche „Chilling“ in verfassungsmäßig missbilligter Art und Weise („negatives Chilling“), wirkt sich dies als Teil der objektiv-rechtlichen Wirkungsdimension der Grundrechte aus. Die Existenz von Chilling Effects beeinflusst somit die Auslegung von *unbestimmten Rechtsbegriffen* und insbesondere die *allgemeinen rechtlichen Abwägungsentscheidungen*, wie z. B. die Verhältnismäßigkeitsprüfung. Darüber hinaus kann eine solche staatliche Einschüchterungsbeeinflussung auch selbst einen Grundrechtseingriff darstellen. Notwendig ist dafür nach der Lehre vom modernen Eingriffsbegriff aber das Überschreiten einer *Spürbarkeitsschwelle*: Nicht *jeder* „Chilling Effect“ ist ein Grundrechtseingriff.

Auch zu Überwachung als Auslöserin von Chilling Effect gibt es Rechtsprechung: Die Gerichte erkennen an, dass Überwachung Chilling Effects auslöst; dies wird auch rechtlich missbilligt.[189] Staatliche Überwachung betrifft bestimmte Grundrechte „einschüchternd“ – in andere Grundrechte greift sie aber *unmittelbar* ein. So ist z. B. die Meinungsfreiheit nur in Form eines „Chilling Effect“ betroffen, in das Telekommunikationsgeheimnis oder das Grundrecht auf informationelle Selbstbestimmung liegen aber konkrete *Eingriffe* vor.

In jedem Fall ist das Ausmaß der „Chilling Effects“ ein relevanter, mit*entscheidender* Punkt der rechtlichen Bewertung staatlicher Massenüberwachung. Denn Überwachung betrifft nicht nur einzelne Bürger, sondern die Gesellschaft als ganzes. Die verschiedenen einschlägigen Grundrechtekataloge, maßgeblich das deutsche Grundgesetz, geben ein System der demokratischen Willensbildung vor, in dem der unbefangene, un-eingeschüchterte Freiheitsgebrauch der Bürger eine zentrale Rolle einnimmt: Die Grundrechtsträger sind die *beweglichen Teile* dieses Kommunikationssystems. Sie sind es, die auf die

[189] Siehe dazu die Hinweise in Abschnitt 1.2.3.

unterschiedlichen Anforderungen der Kommunikationsverfassung reagieren sollen, sie sollen eine gesamtgesellschaftliche Auffassung entwickeln und diese in den Staatsapparat einspeisen. Je freier sie ihre Meinungen äußern, je besser sie Pro und Contra abwägen, je besser sie informiert sind etc., desto besser funktioniert letztlich auch die Demokratie. Es ist diese *Beweglichkeit*, die vor den Chilling Effects geschützt werden muss.

Genau hier wirkt sich Überwachung aber aus: Sie macht Einzelpersonen, die aus der Masse heraustreten, für die Hoheitsmacht erkennbar und schüchtert sie so ein. Dies betrifft insbesondere zwei Personengruppen, die für den öffentlichen, demokratischen Diskurs besonders wichtig sind: Personen mit einer besonders wichtigen Rolle für die öffentliche Meinungsbildung (Meinungsführer) und Vertreter von Minderheitsmeinungen. Gerade diese beiden Gruppen – und vor allem ihre gemeinsame Schnittmenge – sind für die demokratische Meinungsbildung besonders wichtig. Wenn diese Gruppen eingeschüchtert werden, verliert die Gesellschaft ihre Innovations- und Selbsterneuerungsfähigkeit, es leidet letztlich die Allgemeinheit.

Dass die Massenüberwachung, die von *Snowden* enthüllt wurde, sich auf die Bürger einschüchternd auswirkt, ist nachgewiesen. Ebenfalls ist jedenfalls der Anscheinsbeweis erbracht, dass *gerade* die *„Meinungsführer",* gerade die Vertreter von *Minderheitsmeinungen,* besonders betroffen sind. Gerade hieraus ergibt sich eine spürbare Beeinträchtigung nicht nur individueller Rechtspositionen, sondern auch des demokratischen Diskurses als solchem. In rechtlicher Hinsicht greifen also nicht nur die individuellen Kommunikationsgrundrechte, sondern auch die *Kommunikationsverfassung* als Gesamtverbund in Zusammenschau mit dem *Demokratieprinzip*.

Aus welchen Grundrechten bzw. welche Grundrechte*katalogen* die Chilling Effects abgeleitet werden, ist eine Frage der konkreten Fallgestaltung und des

jeweils angewendeten Rechtsverfahrens.[190] Da Geheimdienste verschiedener Staaten international zusammengearbeitet haben, stellt sich einerseits die Frage nach der *internationalen* bzw. *extraterritorialen* Wirkung von Grundrechten; andererseits nach der Zurechnung von Grundrechtsverletzungen. Einen „grundrechtsfreien Raum" gibt es zumindest aus Sicht des deutschen Verfassungsrechts und der deutschen Hoheitsgewalt nicht: Soweit grundrechtsunterworfene Geheimdienste die Grundrechtsverletzungen anderer, nichtunterworfener Geheimdienste geduldet oder sogar gefördert haben, sind ihnen diese zurechenbar.

Angesichts des Ausmaßes der Überwachung und der massiven Chilling Effects, die diese ausgelöst hat, bewegt sich das gesamte Überwachungsprogramm der NSA – bzw. die Teilnahme der deutschen Hoheitsgewalt hieran – vor dem Maßstab des deutschen Grundgesetzes in der Illegalität. Gleiches gilt für die Geheimdienste aller involvierten Europarats-Staaten vor dem Maßstab der EGMR.

[190] Zu einschlägigen Rechtsverfahren *Assion*, Telemedicus v. 26.08.2014, http://tlmd.in/a/2806.

Best Of des Überwachungsrechts - Die Mär vom deutschen Überwachungsstaat?

Jakob Dalby

Internetnutzer treibt eine Frage um: Wer darf wann und wie an meine Daten? Nicht umsonst hat das BVerfG den Passus von einem „diffus bedrohlichen Gefühl des Beobachtetseins“ verfasst. Jedoch scheint es, als habe sich dieses Gefühl mittlerweile verstärkt, hin zu einer diffusen Angst, genährt von einem gefährlichen Halbwissen über die praktischen behördlichen Möglichkeiten und die korrespondierenden rechtlichen Befugnisse. Vorratsdaten, Quellen-TKÜ und Online-Durchsuchung sind Gemeinplätze einer „Verfolgungsparanoia“ geworden.

Zu Recht?

1 Einführung

Der Beitrag befasst sich mit den teils angewendeten, teils diskutierten Ermittlungsinstrumenten der Strafverfolgung. Es werden deren Anwendungsbereich und die rechtlichen Rahmenbedingungen der StPO dargestellt. Hauptaugenmerk liegt hierbei auf den gesetzlichen Voraussetzungen der vorgestellten Maßnahmen unter Berücksichtigung der materiellen und verfahrensrechtlichen Sicherungsmechanismen zum Schutze der Betroffenenrechte. Ziel ist, ein notwendiges Stück Aufklärungsarbeit für eine weiterführende Diskussion zu schaffen.

Zur Einführung werden die Ziele des Beitrags benannt (1.1). Es folgt die Darstellung der Grundlagen der Strafverfolgung im Internet (1.2) mit einer Eingrenzung dieses „schlagwortartigen" Themenfelds (1.2.1). Ziel der digitalen Strafverfolgung im weitesten Sinne ist die Tat- und Täterermittlung und die Erlangung ermittlungsrelevanter Daten (1.2.2) zur Verdachtserhärtung und Anklageerhebung. Unerlässlich und der Strafverfolgung immanent ist der Eingriff in Grundrechte (1.2.3) – diese wirken sich bei der konzeptionellen Ausgestaltung der Maßnahmen des 8. Abschnitts der StPO maßgeblich aus.

Anschließend erfolgt eine Darstellung der Ermittlungsmaßnahmen im Einzelnen (2.). Sie folgt einer Ab- bzw. Aufstufung anhand der verschiedenen Daten (Bestands-, Verkehrs- und Inhaltsdaten) die das Ermittlungsziel bestimmen. Der „Best Of"- Charakter des Beitrags erfasst hierbei die Auskunftsersuchen für Bestands- (2.1) und Verkehrsdaten (2.2) unter Berücksichtigung der Vorratsdatenspeicherung und widmet sich vertieft der Inhaltsüberwachung (2.3.) mit der Online-Streife und Ausforschung sozialer Netzwerke sowie den verschiedenen „Spiel- oder Denkarten" der Telekommunikationsüberwachung (Quellen-TKÜ und Online-Durchsuchung).

Der Beitrag schließt mit einem Fazit und einer rechtswissenschaftlichen Bewertung der derzeitigen Strafverfolgungsrealität. In die Beurteilung eingestellt wird hierbei eine Kritik an der Anwendungsebene – Stichwort „Grundrechtsschutz auf dem Papier".

1.1 Ziel des Beitrags

Die kritische Auseinandersetzung mit der Strafverfolgung im Internet ist nicht erst seit den Datenskandalen und der öffentlichen Wahrnehmung der „Totalüberwachung" der Geheimdienste notwendig. Jede Strafverfolgung, jedes bewusste Erheben, Speichern und Auswerten von Informationen macht einen rechtswissenschaftlichen Diskurs nötig, der nicht nur in seinem Ergebnis in einer profunden und verständlichen Art und Weise in die Mitte der Gesellschaft hineingetragen werden muss. Grundrechte (und Eingriffe in diese) betreffen logisch jeden einzelnen Grundrechtsträger. Wichtig war der Mechanismus der „checks and balances" betrieben durch die staatsbürgerliche Öffentlichkeit, schon immer (Volkszählungsurteil). Nur wird er im Datenzeitalter noch greifbarer. Entweder fühlen sich die Menschen „betroffener", da eine „Daten-" oder „Technik-Askese" kaum noch möglich ist, oder diese Betroffenheit ist gerade aufgrund der Verbreitung öffentlicher Meinungen über alle digitalen Kanäle „spürbarer".

Ergebnis eines Diskurses soll nicht eine Befriedigung gesellschaftlicher Forderungen sein (Stop-Überwachung vs. Mehr-Überwachung) und jeden glücklich machen, sondern vielmehr als Zwischenziel eine Diskussion auf Augenhöhe anstoßen. Zur Wahrnehmung eigener Rechte und Beeinflussung gesellschaftlicher Entwicklungen gehört nämlich ein fundiertes Wissen über die tatsächlichen Voraussetzungen, Ziele und Umsetzung strafverfolgungsbehördlicher Aufgaben. Der Gesetzgeber und die jeweiligen Akteure der Sicherheitsbehörden haben die Bürger in ihren Ängsten und Befürchtungen ernst zu nehmen, müs-

sen von diesen aber gleichermaßen in ihrem Strafverfolgungsinteresse zum Rechtsgüterschutz ernst genommen werden. Wissen und Aufklärungsarbeit auf beiden Seiten ist zwingende Voraussetzung.

Die nachfolgenden Ausführungen sollen hierzu einen Beitrag leisten und das Vertrauen stärken – in die Rechtsgrundlagen wie auch den soeben besungenen Willen zu einer kritischen Auseinandersetzung.

1.2 Strafverfolgung "im Internet"

Die Strafverfolgung im Internet ist nicht bloße Kehrseite der Straftatenbegehung im Internet. „Internetkriminalität" zeichnet sich nämlich nicht allein durch internetspezifische Begehungsformen aus (Cyberbullying, Phishing, Cyber Grooming), sondern vor allem dadurch, dass eine Begehung analoger Grundtaten mit dem „Tatmittel Internet" als Katalysator erfolgt.[1]

1.2.1 Gegenstand und Entwicklung

Die Strafverfolgung im Internet beinhaltet die computer- und internetunmittelbaren Straftaten im engeren Sinne, also solche, die das Tatbestandsmerkmal

[1] Die Terminologie in diesem Bereich ist äußerst verwirrend und mehr als uneinheitlich, es kommt zu Doppelnennungen, Überscheidungen und Umbenennungen, vgl. Bundeslagebild Cybercrime 2011, S. 5 sowie Bundeslagebild Cybercrime 2012, S.3 zum Begriff des Cybercrime – dieses hieß zuvor Bundeslagebild IuK; siehe auch PKS 2012, S. 308 - Tabelle mit Bezug zur IuK-Kriminalität i.e.S. als Teil der Computerkriminalität; LKA Baden-Württemberg Jahresbericht Cyberkriminalität/Digitale Spuren 2012, S. 6 f. zu Internet- und Computerkriminalität, abrufbar unter http://www.polizei-bw.de/Dienststellen/LKA/Documents/2012_Cyberkriminalitaet_Digitale_Spuren.pdf; das BKA verwendet die Begriffe Cybercrime, Internetkriminalität und IuK-Kriminalität (scheinbar) im Austauschverhältnis, vgl. http://www.bka.de/nn_234152/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/internetKriminalitaet__node.html?__nnn=true.

EDV im Straftatbestand aufweisen[2] oder bei denen Elemente des EDV wesentlich für die Tatausführung sind.[3] Daneben erfasst sind im weiteren Sinne alle Straftaten, die mit dem „Tatmittel Internet" begangen oder durch dieses begünstigt werden, also unter Ausnutzung der Informations- und Kommunikationstechnik „Internet".[4] Das „Tatmittel Internet" ist somit das maßgebliche Kriterium für eine Festlegung der verfolgbaren Straftaten.

Der modus operandi auf Täterseite erfährt einen Katalysationseffekt durch das Kommunikationsmedium: E-Mail, Soziale Netzwerke, Darkweb, Usenet, Datenaustausch via FTP, Chat, VoIP, mehrfachgenutzte Cloud. Verfolgbare Straftaten sind also nicht nur computer- bzw. internetspezifische Taten, bei denen die Begehungsform einen Netzbezug aufweist (v.a. Betrugsdelikte). Ebenso kann dies auch ein Kapitaldelikt betreffen, welches mittels Internet verabredet, vorbereitet, nachbereitet oder angepriesen wurde.[5] Der Fokus liegt also auf „nicht-internetspezifischen Straftaten".

Hierneben hat die Strafverfolgung im Internet einen hohen ermittlungstaktischen (analogen) Nutzen bei der Tat- und Täteridentifizierung. Über Daten lassen sich Rückschlusse auf konkrete Tatumstände (Zeit, Ort, Durchführung – Beispiel: Forum Zauberwald[6]) ziehen: Das Internet verliert seine vermeintliche personale Abstraktheit. Die Täteridentifizierung und Beweisführung gelingt

---

[2] So die Statistik des *LKA BW* zur IuK-Kriminalität 2011, S. 6 - dies wären die §§ 202a, b, c, 303a, b, 317, 206 als Straftaten gegen die Vertraulichkeit, Verfügbarkeit und Unversehrtheit von Computerdaten und -systemen und 263a, 265a, 268, 269, 274 StGB als computerbezogene Straftaten.

[3] So das *BKA* im Bundeslagebild Cybercrime 2011, S. 5 – im Bundeslagebild 2012, S. 3 findet sich hingegen bereits wieder eine andere Definition, die vom Sinngehalt jedoch nicht darüber hinausgehen dürfte.

[4] So auch die Definition des *LKA BW* in der Kriminalstatistik 2011, S. 6.

[5] Weitere Beispiele sind die organisierte Kriminalität, BTM-Delikte, Kinderpornographie.

[6] *BGH* Beschluss 16.3.2011, Az. 5 StR 581/10 – von einer Lektüre des Beschlusses wird an dieser Stelle abgeraten, da sehr explizit die konkrete Durchführung eines Sexualdelikts wiedergegeben wird.

kurz gesagt durch eine Strafverfolgung „entlang der Kommunikationswege“. Es ändert sich also auch der modus operandi der Strafverfolgungsbehörden.

1.2.2 Zugriffsgegenstand: Daten jeglicher Art

Zugriffsgegenstand und Ziel sind Daten. Sie stellen selbst ermittlungsrelevante Teilergebnisse dar oder führen zu solchen. Das Internet ist hierbei Fluch und Segen. Probleme macht die Datenflüchtigkeit und -ubiquität unabhängig von Landesgrenzen und über diese hinaus. Die gleichzeitig vorherrschende „Datensammlungswut“ der Diensteanbieter ist hingegen von Vorteil. Datenerhebungs-, Speicherungs- und Verwendungskonzepte sind nicht nur notwendiges Vehikel der Strafverfolgung im Internet, sie sind deren Mittelpunkt.

Insgesamt lassen sich die nachfolgenden Daten unter dem Oberbegriff der Telekommunikationsdaten zusammenfassen. Vorherrschend ist hierbei eine Datenkategorisierung – es gilt regelmäßig: Die Datenkategorie bestimmt die Intensität des Zugriff und des Eingriffs in Grundrechte. Ein Paradigma ist dies jedoch nicht.[7]

1.2.2.1 Bestandsdaten

Bestandsdaten sind Angaben über das Verhältnis des Telekommunikationsdienstleisters und des Nutzers, die zur Begründung, inhaltlichen Ausgestaltung, Änderung oder Beendigung eine Vertragsverhältnisses über Telekommunikati-

[7] Dies wäre nicht realitätsnah. So zeigt es die Neuregelung des manuellen Auskunftsverfahrens auf gesetzeskonzeptioneller Ebene: Demnach ist eine Zuordnung anhand dynamischer IP-Adressen (Verkehrsdaten) mittels der manuellen „Bestandsdaten“-Auskunft gem. § 113 TKG i.V.m. § 100j Abs. 2 StPO möglich. M.E. ist daher die Qualität eines Datums generell nicht nach seiner Begrifflichkeit zu bestimmen, sondern immer unter Berücksichtigung von Ermittlungsziel, -weg und Intensität eines Zugriffs. So kann eine Prämisse wie „Zugriff auf Bestandsdatum = kein Richtervorbehalt“ längst nicht mehr richtig sein, vgl. hierzu *Kugelmann/Dalby*, in: *Roggan/Busch* (Hrsg.), FS Kutscha, S. 105, 121.

onsdienste erhoben werden (§ 3 Nr. 3 TKG), etwa Rufnummer, Vertragsbeginn oder statische IP-Adresse. Sie beschränken sich auf den Vertragskunden des Unternehmens.

1.2.2.2 Verkehrsdaten

Verkehrsdaten sind gem. § 3 Nr. 30 TKG solche, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Es handelt sich um Daten, die zum Aufbau und zur Aufrechterhaltung von Telekommunikation benötigt werden.[8] Hierunter fallen mithin auch die wichtigsten Verkehrsdaten für die Strafverfolgung im Internet, die dynamischen IP-Adressen.[9]

1.2.2.3 Inhaltsdaten

Diese sind aussagekräftigsten Daten aus Nutzer- und Behördensicht. Inhaltsdaten beschreiben konkrete Inhalte zwischenmenschlicher Telekommunikation; sie sind menschlich wahrnehmbar und werden zwischen Nutzern ausgetauscht.[10] Sie müssen jedoch nicht zwingend Gegenstand eines direkten persönlichen Austauschs zwischen mind. zwei Personen sein. Inhaltsdaten sind auch solche, die der Nutzer selbst kreiert (Bsp. E-Mails im Entwurfsstadium, Kochrezepte auf dem Heim-PC, Online-Tagebuch, Dokumente in der Cloud).

---

[8] *Graf,* in: Beck-OK StPO, Ed. 17 2014, § 100a Rn. 1 f.; *Büttgen,* in: *Hoeren* et al., Multimediarecht, 35. Aufl. 2013, Teil 16.3. Rn. 93 ff. Beispielsweise Daten von wann bis wann eine Konnektivität mit dem Internet bestand.

[9] Vgl. statt vieler *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, Rn. 701; mit Nachweisen über die Beurteilung des Gesetzgebers als Bestandsdatum, *Sankol* MMR 2008, 480. Oft verkannt wird, dass eine dynamische IP-Adresse zwar beim Verbindungsaufbau anfällt und damit Verkehrsdatum ist, aber dennoch einem „technischen und rechtlichen Nullum" gleichkommt (*AG Offenburg*, 4 Gs 442/07, Rn. 29). Erst die Zuordnung zum Nutzer unter Eingriff in Art. 10 GG verleiht ihr Gewicht. Eine Einordnung als „qualitatives Bestandsdatum" drängt sich auf. Diesen Schluss legt nun auch der neue § 113 TKG nahe, vgl. hierzu *Dalby* CR 2013, 361, 364 f.; im Ergebnis auch *Graf,* in Beck OK-StPO, § 100j, Rn. 19a.

[10] *Gercke/Brunst* (Fn. 9), Rn. 636.

1.2.3 Bedeutung der Grundrechte

Der Schutz vorgenannter Daten ist zwingend. Zum einen, da diese zumeist personenbezogen sind,[11] zum anderen, da der staatlichen Kenntnisnahme eine Ermittlungsmaßnahme vorhergeht, die den Betroffenen zum Gegenstand von Strafverfolgung macht.[12] Es kommt zu Eingriffen in Grundrechte. Insofern trifft zu, dass unter den Bedingungen der automatischen Datenverarbeitung kein "belangloses" Datum mehr existiert.[13]

1.2.3.1 Recht auf informationelle Selbstbestimmung

Sachlich schützt es den Kernbereich der privaten Lebensgestaltung und ist Ausformung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. [14] Es stellt dessen notwendige Weiterentwicklung dar und begegnet den Gefahren der automatisierten Datenverarbeitung.[15] Es beinhaltet das Recht, über die Preisgabe und Verwendung persönlicher Daten in informationell selbstbestimmender Weise zu entscheiden.[16] Bestandsdaten und Inhaltsdaten stehen unter dessen Schutz.[17] Ein Eingriff liegt immer dann vor, wenn persönliche Daten von einem Dritten ohne Einwilligung offenbart wer-

---

[11] Bei der dynamischen IP-Adresse str., da es sich hier eigentlich nur um eine Nummernfolge handelt, die einen konkreten Personenbezug i.S.d. § 3 Abs.1 BDSG erst durch eine Zuordnung und Verknüpfung erhält. Der *BGH* legt diese Frage dem *EuGH* vor, Beschl. v. 28.10.2014, Az. VI ZR 135/13.

[12] Dies sind etwa Auskunftsverfahren bzgl. Bestandsdaten, Beschlagnahme von Computern oder E-Mail-Postfächern oder eine heimliche Telekommunikationsüberwachung durch das Abfangen von Rohdaten.

[13] *BVerfG* NJW 1984, 419, 422.

[14] *Herdegen,* in: *Maunz/Dürig*, GG, 69. Aufl. 2013, Art. 1, Rn. 84.

[15] Entwickelt durch das *BVerfG*, Urt. vom 15.12.1983 = *BVerfG* NJW 1984, 419.

[16] *BVerfG* NJW 1984, 422, vgl. auch *Weichert,* in: *Kilian/Heussen*, Computerrechts-Handbuch, 31. Aufl. 2012, Rn. 4. Dies betrifft alle persönlichen Lebenssachverhalte, unabhängig von der Zuordnung zur Privat- oder Intimsphäre und der Sensibilität der Daten.

[17] *Kugelmann/Dalby* in *Roggan/Busch* (Fn. 7), S. 105, 109 – Inhaltsdaten können natürlich auch unter dem Schutze des Art. 10 GG stehen, wenn es spezieller ist.

den. Dies meint die Erhebung, Sammlung, Speicherung, Verwendung und Weitergabe der Daten.[18]

1.2.3.2 Telekommunikationsgeheimnis

Das Telekommunikationsgeheimnis des Art. 10 GG wird aufgrund des Verlustes von Herrschaftsgewalt über Informationen durch neue Medien mittlerweile als einheitliches, technikoffenes Telekommunikationsgrundrecht verstanden.[19] Sachlich umfasst ist Kommunikation, bei der es um den unkörperlichen Austausch von Gedankeninhalten zwischen zwei Personen unter Mitwirkung eines Dritten, des Kommunikationsmittlers (Telekommunikationsdiensteunternehmen), geht („entwicklungsoffenes Auffanggrundrecht").[20] Alle Kommunikationsdienste des Internets sind erfasst.[21] Geschützt werden die Inhalte und Umstände des Kommunikationsvorgangs (Ort, Zeit, Art und Weise der Kommunikation, z. B. die zur Zuordnung dynamischer IP-Adressen notwendigen Informationen,[22] Beteiligte, Dauer und Häufigkeit). Dies umfasst logisch die Verkehrsdaten.[23] Inhaltsdaten können sowohl durch Art. 10 GG wie auch durch das Recht auf informationelle Selbstbestimmung des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützt sein.[24] Ein Eingriff erfolgt bei jeder „Kenntnisnahme, Aufzeichnung und Verwertung"[25] und anschließender Speicherung.[26]

---

[18] *Lang*, in: Maunz/Dürig, Art. 2, Rn. 176.
[19] *BVerfG* NJW 2002, 3619, 3620.
[20] *Durner,* in: Maunz/Dürig, Art. 10, Rn. 81.
[21] *Bär*, TK-Überwachung, § 100a StPO, Rn. 4. Erfasst ist generell jede Telekommunikation (Kabel oder Funk, analoge oder digitale Vermittlung) und jede verwendete Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten), *BVerfG* NJW 2002, 3619.
[22] *BVerfG* NJW 2012, 1419, 1422.
[23] *Durner,* in: Maunz/Dürig, Art. 10, Rn. 85.
[24] Vgl. *Baldus,* in: Beck-OK GG, Ed. 19 2013, Art. 10, Rn. 42; *Gersdorf,* in: Beck-OK Medienrecht, Ed. 2 2013, Art. 2 GG, Rn. 87. Der Terminus „Inhaltsdatum" ist also nicht maßgeblich für die Schutzdimension. Nur weil ein Inhaltsdatum Gegenstand und Ziel einer Maßnahme ist, bedeutet dies nicht die Betroffenheit eines

1.2.3.3 IT-Grundrecht[27]

Das IT-Grundrecht schuf das BVerfG erneut aus der Notwendigkeit veränderter gesellschaftlicher Umstände.[28] Es ist Variante des Rechts auf informationelle Selbstbestimmung und hat seine Wurzeln ebenfalls in Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG. Grund war die Erkenntnis, dass das Recht auf informationelle Selbstbestimmung der veränderten Nutzung informationstechnischer Systeme zur Persönlichkeitsentfaltung nicht ausreichend Rechnung trägt. Ein solches System erhebt notwendig personenbezogene Daten, es entsteht ein zugriffsgefährdeter „aussagekräftiger Datenbestand".[29]

Geschützt wird nunmehr das informationstechnische System selbst zur Gewährleistung von dessen Vertraulichkeit und Integrität.[30] Hierzu zählen alle „Devices" (PC, Laptop, Smartphones) sowie deren Vernetzung. Maßgeblich ist, ob das System des Geräts Daten in einer solchen Menge verarbeitet und speichert, dass diese Aufschluss über wesentliche Teile der Lebensgestaltung ermöglichen.[31] Geschützt sind die Daten im Arbeitsspeicher sowie alle temporär oder dauerhaft vorhanden Daten in anderen Speichermedien des Systems. [32] Der Schutz umfasst jedoch nur das „eigengenutzte" informationstechni-

---

bestimmten Grundrechts (bspw. Art. 10 GG. Insofern unterscheidet sich die Kategorisierung hier von derjenigen als Bestands- oder Verkehrsdatum.

[25] *BVerfG* NJW 1992, 1875, 1876.

[26] Jede Weitergabe und Weiterverwendung der Kommunikationsdaten stellt einen erneuten Eingriff dar. Für eine Aufzählung der verschiedenen Eingriffe siehe *Baldus*, in: Beck-OK GG, Art. 10, Rn. 27.

[27] Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, teils auch Computergrundrecht genannt, was allerdings missverständlich ist, da jedes IT-System gemeint ist, korrekt wäre also die Bezeichnung „IT-System-Grundrecht".

[28] Urteil zur Online-Durchsuchung vom 27.02.2008, *BVerfGE* 120, 274 = *BVerfG* NJW 2008, 822.

[29] *BVerfG* a.a.O., 827.

[30] *Skistims/Roßnagel*, ZD 2012,3, 5.

[31] *BVerfG* NJW 2008, 822, 827.

[32] *BVerfG* a.a.O.

sche System.[33] In Schutzrichtung des Persönlichkeitsrechts trägt nur dessen Systeminhalt persönlichkeitsrelevante Elemente des Kernbereichs der privaten Lebensgestaltung. Ein Eingriff liegt auch hier bei Erhebung, Sammlung, Speicherung, Verwendung und Weitergabe von Daten vor, die durch einen Zugriff auf das informationstechnische System erlangt wurden, insbesondere wenn dieser heimlich erfolgt (Vertraulichkeit). Ein solcher liegt auch vor bei Zugriffen auf Leistungen, Funktionen und Speicherinhalte (Integrität). Die „Hürde für eine Ausspähung, Überwachung oder Manipulation" des gesamten Systems ist dann genommen.[34]

1.3 Grenzen? - "Die heißen Eisen"

Das Terrain, auf dem sich eine grundrechtskonforme Gesetzgebung und ein verhältnismäßiges Handeln der Strafverfolgungsbehörden bewegt, sollte nun hinreichend beschrieben sein.

Aus dem Spannungsverhältnis „Strafverfolgungsinteresse & Rechtsgüterschutz vs. Grundrechte & Status Negativus" sollten keine „Denkverbote" entstehen. Ein kategorischer Ausschluss bestimmter Ermittlungsmaßnahmen ist für einen ergebnisorientierten Diskurs in dem sich alle Akteure gleich ernst nehmen, kontraproduktiv. Die emotionale Bandbreite, die sich während des Vortrags bei der Nennung der Begriffe „Vorratsdatenspeicherung" oder „Online-Durchsuchung" in den Gesichtern der interessierten Zuhörer/innen abspielte, verdeutlichte dies.[35] Austausch und Information, quasi Öffentlichkeitsarbeit,

[33] Vgl. zu dieser semantischen Abänderung sehr interessant *Hoffmann-Riem* JZ 2008, 1009, 1020. Nicht „eigengenutzt" sind somit Cloud Ordner, in denen durch mehrere Nutzer Daten abgelegt werden – bspw. Share-Funktion bei Dropbox.
[34] *BVerfG* a.a.O., 825.
[35] Die negative Konnotation konnte durch deutliche Reaktionen auch bei Diskussionen und Vorträgen im Zuge der Tagung festgestellt werden. Verwunderlich ist in diesem Zusammenhang eine Studie des Deutschen Instituts für Wirt-

müssen den Diskurs entemotionalisieren. Die negative Belegung bestimmter Schlagworte rührt nicht von ungefähr. Doch sollte eine Ermittlungsmaßnahme nicht per se verteufelt werden. Ohne Widerspruch darf sich dies aber auf die konkrete *Umsetzung* beziehen, in gesetzeskonzeptioneller wie praktischer Hinsicht (siehe dazu unten Abschnitt 3. – Fazit).

Sollte sich herausstellen, dass eine Ermittlungsmaßnahme wie die Quellen-TKÜ grundrechtskonform umsetzbar ist, muss dies von deren Gegnern toleriert werden. Der Gesetzgeber und die Strafverfolgungsbehörden müssen ebenso tolerieren, wenn selbiges für eine Online-Durchsuchung nicht gilt.

Zu den „heißen Eisen" gehören die Vorratsdatenspeicherung, die Online-Durchsuchung, die Quellen-TKÜ und im weitesten Sinne auch die Beschlagnahme von großen Datenbeständen wie z. B. Facebook-Accounts und ganzer E-Mail-Postfächer.[36] Die Argumente und Gegenargument müssen im hellen Schein der Grundrechte sorgsam abgewogen werden, eben hierauf beruht eine grundrechtskonforme und -schützende Umsetzung.

---

schaft aus 2014, wonach 2 von 3 Bürgern gegen eine Vorratsdatenspeicherung sind, 70 % Fluggastdatenspeicherung aber befürworten; abrufbar unter http://www.diw.de/de/diw_01.c.479846.de/themen_nachrichten/zwei_von_drei_buergern_lehnen_vorratsdatenspeicherung_ab.html. Allerdings rekurriert die Studie auf eine Befragung aus 2011, also noch vor dem NSA-Skandal.

[36] Auf letztere Aspekte kann hier nur exkursmäßig eingegangen werden. Ergebnisse lassen sich aber übertragen. Eine Beschlagnahme eines Facebook-Accounts richtet sich m.E. offen nach den §§ 94 ff. StPO und verdeckt nach § 100a StPO. Letzteres beruht auf den Ausführungen, die auch für E-Mail-Accounts zutreffen (s.u.).

2 Die Ermittlungsmaßnahmen im Internet

Die vorgestellten Datenkategorien ermöglichen bereits einen ersten Fingerzeig auf einschlägige Rechtsgrundlagen. Zwischen Inhalts-, Verkehrs- und Bestandsdaten besteht in der Regel eine Abstufung hinsichtlich der Eingriffsintensität in Grundrechte des Betroffenen.[37] Aber nicht nur die Datenkategorie bestimmt über die Ermittlungsmaßnahme und Eingriffsintensität, sondern auch der Zugriffsweg und die Modalitäten des Zugriffs.[38] Die Ermittlungsmaßnahmen sind (auf dem Papier) in ihrer Ausgestaltung an die Grundrechtsrelevanz und Eingriffsintensität angepasst. Jedenfalls trifft dies auf ihre gesetzestechnische Ausgestaltung zu. Die praktische Wirksamkeit materiell begrenzender Tatbestandshürden und verfahrenstechnischer Sicherungsmechanismen „steht auf einem anderen Blatt".[39]

[37] Anders bei Zugangssicherungsdaten, die als Bestandsdaten einzuordnen sind. Über diese kann auf denkbar einfachstem Weg der Zugang zu Inhaltsdaten eröffnet werden (bspw. Passwort des Dropbox-Accounts öffnet diesen zum Download aller Daten). Diese Bestandsdatenabfrage ist von erheblicher Eingriffsintensität (s.u.).

[38] Zur Notwendigkeit einer Gesamtschau bei der Bestimmung der Eingriffsintensität in Grundrechte bei Datenzugriffen, *Kugelmann/Dalby,* in: *Roggan/Busch* (Fn. 7), S. 105, 120 f.

[39] Siehe hierzu auch das Fazit unter 3.

2.1 Bestandsdatenabfrage

Stark frequentiert werden das automatisierte und manuelle Auskunftsverfahren des TKG. Durch diese wird eine Personenidentifizierung ermöglicht. An die erlangten Informationen können weitere Ermittlungen anknüpfen.[40]

2.1.1 Das automatisierte Auskunftsverfahren gem. § 112 TKG

Die Bedeutung des automatisierten Auskunftsverfahrens zeigen „nackte Zahlen“:[41] Ca. 102 registrierte Sicherheitsbehörden können bei 127 TK-Unternehmen Bestandsdaten abrufen. So erfolgten im Jahr 2013 7 Mio. Ersuchen an die Bundesnetzagentur, die anschließend 35,2 Mio. Abfragen bei den beteiligten Telekommunikationsdiensteunternehmen vornahm.[42]

2.1.1.1 Gegenstand und Durchführung

Gegenstand ist die Abfrage von Bestandsdaten des § 111 TKG. Verpflichtet zur Speicherung dieser Daten sind Unternehmen, die öffentlich zugängliche Telekommunikationsdienste anbieten.[43] Diese müssen die in § 111 Abs. 1 TKG genannten Daten erheben (Name des Anschlussinhabers, Geburtsdatum, E-Mail-Adresse, statische IP-Adressen sind m.E. nicht erfasst)[44], in einer Kunden-

---

[40] Beispiel: Steht fest, unter welcher E-Mail-Adresse der Beschuldigte erreichbar ist, kann der E-Mail-Account beschlagnahmt werden.

[41] „AutomatsiertAutomatisiert“, da die Anfragen an die Bundesnetzagentur gehen, die dann Abfragen über die Datenbänke der Diensteunternehmen macht.

[42] Jahresbericht Bundesnetzagentur 2013, S. 98 f.

[43] Ausgeschlossen sind z. B. Universitätsnetze, Internetcafés, Firmennetzwerke.

[44] *Gercke/Brunst* (Fn. 9), Rn. 677. Statische IP-Adressen werden teils unter „andere Anschlusskennungen“ gefasst, str.: für andere Anschlusskennungen *Eckhardt,* in: *Geppert/Schütz* (Hrsg.), Beck’scher TKG-Kommentar, 4. Aufl. 2013, § 111 TKG, Rn. 13, der statische IP-Adressen als erfasst betrachtet, dynamische IP-Adressen hingegen nicht. Es ist aber schon der Gesetzesbegründung nach ein enges Verständnis des Begriffs angezeigt, siehe BT-Drs. 16/5846, S. 68. Dies ist vor allem vor dem Hintergrund der Einführung der IPv6 wichtig. Die IPv6 ermöglicht die Vergabe von weitaus mehr statischen IP-Adressen als bisher der

datei speichern und der Bundesnetzagentur zum automatisierten Abruf bereit halten. Diese leitet die Daten an die Strafverfolgungsbehörden weiter (§ 111 Abs. 1 S. 5 Nr. 1, Abs. 2 TKG).

2.1.1.2 Voraussetzungen

Das BVerfG bestätigte mit Beschluss vom 24.01.2012 die Verfassungsmäßigkeit der Ausgestaltung des manuellen Auskunftsverfahrens.[45]. Zum Abruf bedarf es im Rahmen des Gesetzesvorbehalts aber einer zugrundeliegenden spezialgesetzlichen Abrufbefugnis (sog. Doppeltürmodell).[46] Der § 112 TKG ist lediglich datenschutzrechtliche Öffnungsklausel (erste Tür) und nicht bereits Ermächtigungsgrundlage zum Abruf. Die Ermittlungsgeneralklausel (§§ 161, 163 StPO) stellt diese Ermächtigungsgrundlage als allgemeine Datenerhebungsbefugnis (zweite Tür) dar.[47]

2.1.2 Das manuelles Auskunftsverfahren gem. § 113 TKG i.V.m. § 100j StPO

2.1.2.1 Gegenstand und Durchführung

Über § 113 TKG sind neben den Daten aus § 111 auch solche gem. § 95 TKG erfasst. Diese gewöhnlichen Bestandsdaten werden explizit ergänzt um geson-

---

Fall. Hierüber wäre dann u.U. möglich, nicht nur konkrete Anschlüsse zu erfassen, sondern einzelne Geräte mit statischen IP-Adressen zu versehen. Das „Internet der Dinge“ würde dann über die statischen IP-Adressen weite Teile der persönlichen Lebensgestaltung nachvollziehbar machen.

[45] *BVerfG* Urteil vom 24.01.2012, 1 BvR 1299/05. Die Speicherung der Bestandsdaten in Kundendateien gem. § 111 TKG, wie auch der Abrufmechanismus des § 112 TKG, genügen demnach den Anforderungen an einen Grundrechtseingriff in das Recht auf informationelle Selbstbestimmung.

[46] *BVerfG* Urteil vom 24.01.2012, 1 BvR 1299/05, Rn. 123.

[47] So auch *Bär* MMR 2013, 700, 702; das *BVerfG* scheint sich in seinem Beschluss zu sträuben dies explizit zu benennen, obwohl hieran kein Zweifel besteht. Der neue § 100j StPO stellt zumindest in Bezug auf Bestandsdaten, die nicht Zugangssicherungsdaten oder dynamische IP-Adressen sind, keine höheren Anforderungen als die Ermittlungsgeneralklausel.

dert genannte Zugangssicherungsdaten. Gänzlich neu eingeführt wurde die Aufnahme der dynamischen IP-Adressen. Auch in Bezug auf das manuelle Auskunftsverfahren gilt das Doppeltürmodell, also das Erfordernis einer spezialgesetzlichen Abrufnorm.[48] § 113 TKG ist ebenfalls nur datenschutzrechtliche Öffnungsklausel und erstarkt erst durch § 100j StPO zu einer Übermittlungsverpflichtung (§ 113 Abs. 4 TKG).[49] Die in § 113 Abs. 3 TKG benannten Sicherheitsbehörden sind zum Ersuchen um Auskunft berechtigt. Das Ersuchen ist manuell, da es direkt an das Telekommunikationsdiensteunternehmen gestellt wird.[50] Weitere Verfahrensvoraussetzungen sind zu erfüllen, dies sind Mitteilungspflichten bei der Beauskunftung anhand dynamischer IP-Adressen gem. § 100j Abs. 4 StPO und der Richtervorbehalt bei der Beauskunftung über Zugangssicherungsdaten gem. § 100j Abs. 5 StPO.[51]

2.1.2.2 Voraussetzungen

Der Zugriff auf die Daten der §§ 95, 111 TKG ist von geringer Intensität. Es kommt „nur" zu einem Eingriff in das Recht auf informationelle Selbstbestimmung.[52] Verfahrenssichernde Elemente sind nicht notwendig.

---

[48] Ausführlich zu § 113 TKG unter kritischer Beurteilung der Ausgestaltung *Dalby* CR 2013, 361; *Kugelmann/Dalby*, *Roggan/Busch* (Fn. 7), S. 105 ff.

[49] Andere fachgesetzliche Abrufnormen wurden mit der Gesetzesnovelle (BGBl. I 2013, 1602) ebenfalls geändert oder eingefügt, die Folgeänderungen betreffen: §§ 7, 20b, 20w und 22 BKAG, § 22a BPolG, §§ 7, 15 ZFdG, § 8d BVerfschG, § 2b BNDG, § 4b MAD-G.

[50] Der Kreis der Verpflichteten ist größer als beim manuellen Auskunftsverfahren (Eingrenzungsmerkmal „öffentlich zugänglich" fehlt). Es sind auch interne Netze wie Universitäts- oder Firmennetze erfasst.

[51] Ausführlich zum Richtervorbehalt *Kugelmann/Dalby*, in: *Roggan/Busch* (Fn. 7), S. 105, 115 ff.

[52] *BVerfG* NJW 2012, 1419, 1422. Über § 95 TKG werden statische IP-Adressen erfasst. Dynamische IP-Adressen fallen hingegen weder unter § 111 TKG, noch unter § 95 TKG. Nichtsdestotrotz sind sie von einer Auskunft nach § 113 TKG umfasst. Der Terminus „Bestandsdatenauskunft" ist also fehlgehend, da sie mit der Novelle zu einer partiellen Verkehrsdatenauskunft geworden ist. Zur Rechtmäßigkeit einer Speicherung dynamischer IP-Adressen, s.u. 2.2.1.1.

§ 113 Abs. 1 S. 3 TKG i.V.m. § 100j Abs. 1 S. 1, Abs. 2 StPO[53] beinhaltet dem Wortlaut nach die Zuordnung einer dynamischen IP-Adresse zu identifizierenden Bestandsdaten und die Auskunft hierüber „anhand" der dynamischen IP-Adresse. Dogmatisch spricht auch nichts gegen die umgekehrte Auskunft „über" eine verwendete dynamische IP-Adresse.[54] Gegenstand ist die Mitteilung der zuvor unbekannten IP-Adresse anhand des Namens, der Uhrzeit und des Anschlusses des bereits bekannten Verwenders. Es kommt auch hier zum Einblick in konkrete Telekommunikationsverbindungen und Kenntnisnahme weiterer Verkehrsdaten[55]: Der Provider muss feststellen, zu welchem Zeitpunkt die dynamische IP-Adresse zugeordnet war. Ein Eingriff in Art. 10 GG liegt vor. Diese gesteigerte Eingriffstiefe erfordert (mindestens) die fachgesetzlich geregelte Mitteilungspflicht an den Betroffenen (§ 100j Abs. 4 S. 1 Var. 2 StPO).

Kritisch ist, dass ein Richtervorbehalt in Bezug auf dynamische IP-Adressen fehlt. Ein Eingriff in Art. 10 GG muss durch einen Richtervorbehalt abgefedert werden.[56] Die Benachrichtigungspflicht allein trägt dem Gefährdungspotential des Eingriffs in Art. 10 GG nicht ausreichend Rechnung. Die verfahrenssichernden Maßnahmen würden mit einem Richtervorbehalt auf das Niveau des § 100g StPO, also das der Verkehrsdatenabfrage gehoben. § 113 Abs. 1 S. 3 TKG i.V.m.

---

[53] Abs. 2 verweist ohne Satzbezeichnung auf Abs. 1. Da der Gesetzgeber die Anforderungen der Beauskunftung dynamischer IP-Adressen wohl nicht an die Voraussetzungen der Abfrage von Zugangsdaten aus S. 2 knüpfen wollte, ist § 100j Abs. 1 S. 1 StPO einschlägig. So bereits *Dalby* CR 2013, 361, 365, zustimmend *Bär* MMR, 700, 703.

[54] Der Zugriffsweg unterscheidet sich bei der Identifizierung der dynamischen IP-Adresse nicht vom Fall (Zuordnung „anhand" dynamischer IP-Adresse). Hier wie dort kommt es zum Einblick in Umstände der Telekommunikation. Vgl. *Dalby* CR 2013, 361, 365; zustimmend *Graf*, in: Beck-OK StPO, § 100j Rn. 19a, zustimmend auch *Bär* MMR 700, 703. Anders ein Großteil der Literatur (m.w.N. *Gercke/Brunst* (Fn. 9), Rn. 663 ff vor Änderung des § 113 TKG) wonach die Zuordnung anhand der dynamischen IP-Adresse unter § 100g StPO fallen sollte.

[55] Zuletzt *BVerfG* NJW 2012, 1419, 1422.

[56] So bereits *Kugelmann/Dalby,* in: *Roggan/Busch* (Fn. 7), S. 105, 115.

§ 100j Abs. 1, S. 1, Abs. 2 StPO wäre in der Strenge der Zugriffsvoraussetzungen zwischen Bestandsdatenauskunft und Verkehrsdatenabfrage anzusiedeln.[57]

Für Zugangssicherungsdaten (Passwörter, PINs und PUKs zu Endgeräten und in diesen eingesetzte oder von diesen räumlich getrennte Speichereinrichtungen) sind die Zugriffvoraussetzungen gem. § 113 Abs. 1 S. 2 TKG i.V.m. § 100j Abs. 1. S. 2 StPO nachvollziehbar am Höchsten. Hiervon umfasst sind laut Gesetzesbegründung zutreffender Weise auch Cloud-Dienste.[58] Entsprechend den Vorgaben des BVerfG wird die Auskunft über diese Daten an die Voraussetzungen des Nutzungszwecks geknüpft.[59] Da sie mittelbar den Zugriff auf die konkreten Inhalte eines Endgeräts oder einer Speichereinrichtung ermöglichen, ist dies konsequent: Warum sollten die Voraussetzungen für einen Zugriff auf ein

[57] Im Ergebnis wohl auch *Bär*, der weder § 113 TKG noch § 100g StPO als passend ansah – zugegebenermaßen zeitlich vor Neufassung des § 113 TKG, vgl. TK-Überwachung, § 100g, Rn. 27.

[58] BT-Drs. 17/12879, S. 17. In aller Kürze: Dies trifft entgegen neuerer Ansichten (vgl. *Wicker* MMR 2014, 298 ff.) zu, da Cloud Storage-Dienste als typengemischte Verträge im Schwerpunkt einem Werkvertrag zuzuordnen sind. Die jederzeitige Datenverfügbarkeit ist „Versprechen" des Anbieters. Dies wirkt sich auch auf die telekommunikationsrechtliche Einordnung aus. Cloud-Dienste können sowohl unter das TMG und das TKG fallen. Aus Nutzersicht tritt der Cloud-Anbieter als Zugangsanbieter auf. Dem Nutzer ist nicht erkennbar, wer für die Konnektivität verantwortlich ist, der Cloud-Anbieter verspricht und garantiert sogar werbewirksam die Ausfallsicherheit. Hieran muss er sich festhalten lassen. Dies gilt vor allem vor dem Hintergrund einer Virtualisierung der Cloud-Plattformen. Die Bestandsdaten des Cloud-Nutzers werden nämlich zum Transport der Daten vom Server zum Nutzer benötigt, mithin zum Zweck der Erbringung eines Telekommunikations- und nicht eines Telemediendienstes gespeichert (vgl. § 3 Nr. 3 TKG). Dies ergibt sich im Übrigen auch aus dem Vergleich mit der E-Mail-Übertragung, für E-Mail Dienste gilt das TKG, vgl. RRL 2002/21/EG, Erwägungsgrund 10. Eine andere Beurteilung des Cloud-Anbieters, der auch fremde Daten in eigener Herrschaftssphäre vorhält, wäre nicht verständlich. Sie kann nicht nur an dem Merkmal einer Individualkommunikation scheitern, schließlich liegt „Telekommunikation" zwischen Client- und Cloud-Server im Zwei-Personen-Verhältnis vor.

[59] *BVerfG*, Beschluss vom 24.01.2012, 1 BvR 1299/05, Rn. 185.

Passwort andere sein, als für einen Zugriff auf die Daten direkt?[60] Die Abfrage ist verfahrensrechtlich damit nicht nur an einen Richtervorbehalt geknüpft (§ 100j Abs. 3 StPO), sondern zusätzlich an die Voraussetzungen gebunden, die bezogen auf den in der Abfragesituation konkret erstrebten Nutzungszweck bestehen (ggf. schwere Straftat, weiterer Richtervorbehalt).[61] Dieses Erfordernis kann man als Etablierung einer „dritten Tür" bezeichnen.[62]

2.2 Verkehrsdatenabfrage und Vorratsdatenspeicherung

2.2.1 Verkehrsdatenabfrage gem. § 100g StPO

Die Verkehrsdatenabfrage dient zur Ergänzung der Ergebnisse, die aus §§ 112, 113 TKG gewonnen wurden: „Wann" ein Beschuldigter „wo" „wie" mit „wem" kommunizierte.

2.2.1.1 Gegenstand und Durchführung

Die von § 100g StPO erfassten Daten werden durch Verweis auf die §§ 113a, 96 TKG nochmals eingegrenzt, wobei § 113a TKG nach Rechtsprechung des BVerfG verfassungswidrig ist.[63] Umfasst sind gem. §§ 96 ff. TKG u.a. Nummer und

---

[60] Für den Zugriff auf das Passwort zum E-Mail-Account (sofern nicht nur als Hash-Wert vorliegt) gelten dieselben Voraussetzungen wie für das heimliche Auslesen des Accounts. M.E. ist dies § 100a StPO und nicht etwa die Beschlagnahmevorschriften der §§ 94 ff. oder § 99 StPO; s.u.

[61] *BVerfG* NJW 2012, 1419, 1430. Es hat aber keine doppelte richterliche Entscheidung zu erfolgen.

[62] So bereits *Dalby* CR 2013, 361, 364.

[63] Das *BVerfG* erklärte § 113a TKG und § 113b TKG mit Urteil vom 2.3.2010 als verfassungswidrig, vgl. *BVerfG*, Urteil vom 02.03.2010 - 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08; *BVerfGE*, 124, 260 = *BVerfG* NJW 2010, 833. Die Verweisung des § 100g Abs. 1 StPO auf § 113a TKG ist damit obsolet. § 100g StPO als Zugriffsregelung wurde seinerseits für verfassungswidrig erklärt und ist teilnichtig.

Kennung des Anschlusses oder der Endeinrichtung, bei Mobilgeräten auch die Standortdaten, Beginn und Ende der Verbindung und zum Aufbau und Aufrechterhaltung der Verbindung dienende Daten.[64]

Streitig ist nach wie vor, ob die §§ 96 ff. TKG die Diensteanbieter zur Erhebung und Speicherung dynamischer IP-Adressen ermächtigen. Sie geben Aufschluss, wann über welchen Anschluss gesurft wurde und ermöglichen über § 113 Abs. 1 S. 2 TKG die Ermittlung des hinter der dynamischen IP-Adresse stehenden Vertragskunden. Der Gesetzgeber scheint von der Rechtmäßigkeit auszugehen, anders lässt sich nicht erklären, warum er im neuen § 113 TKG eine Zuordnung anhand dynamischer IP-Adressen regelt.[65] Zu beachten ist aber, dass IP-Adressen durch die Flatrate-Verbreitung zu Abrechungszwecken weder „erforderlich" sind,[66] noch ermächtigt § 100 TKG den Diensteanbieter, diese „anlasslos" zum Zwecke der Beseitigung von Störungen und Fehlern vorzuhalten.[67] Insbesondere letzteres wird gem. § 96 Abs. 1 S. 1 Nr.1, S. 2 i.V.m. § 100 Abs.1 TKG (wohl) von den meisten Anbietern praktiziert und führt zu einer Speicherberechtigung von mindestens 7 Tagen.[68] Einer anlasslosen und damit unrecht-

---

[64] Nur Anbieter öffentlicher Telekommunikationsdienste sind verpflichtet: Universitäten, Bibliotheken, betriebsinterne Netze, Internetcafés etc. sind nicht erfasst.

[65] Im Widerspruch hierzu steht der ursprüngliche § 113a TKG. Der FDP-Entwurf zum Quick-Freeze-Verfahren nahm die Einführung einer Speicherberechtigung auch auf, abrufbar unter http://wiki.vorratsdatenspeicherung.de/images/DiskE_.pdf, siehe § 113a Abs. 2 Nr. 1 TKG-E.

[66] Gem. 96 Abs. 1 Nr. 1 i.V.m 97 Abs. 1, Abs. 2 Nr. 1, Abs. 3 S.1 TKG, vgl. *Brunst* DuD 2001, 618, 619.

[67] Siehe zu Abrechungszwecken *Braun,* in: *Geppert/Schütz* (Fn. 45), § 96 Rn. 7, *Schmitz,* in: *Hoeren* et. al (Fn. 8), Teil 16. 2, Rn. 255 ff.; *Gercke/Brunst* (Fn. 9), Rn. 767 ff.; zur Störungsbeseitigung siehe v.a. *BGH*, Urt. v. 13. 1. 2011 – III ZR 146/10 = *BGH* NJW 2011, 1509, sehr ausführlich auch *Breyer* MMR 2011, 573.

[68] *BVerfG* NJW 2011, 1509, 1511. Vodafone war von dieser Praxis zumindest in einem Fall abgewichen, mit dem Hinweis, dass eine Speicherung dynamischer IP-Adressen über die Verbindung hinaus nicht notwendig sei, vgl. http://www.loschelder.de/de/rechtsanwaelte/aktuelles-rechtsfragen/

mäßigen Speicherung muss aber deutlich widersprochen werden. Sie stellt einen schwerwiegenden Grundrechtseingriff dar, der auf Basis des § 100 TKG nicht gerechtfertigt werden kann.[69] Selbst wenn auf eine Verwendung zu Strafverfolgungszwecken nicht abgezielt wird, ist die Speicherung geeignet, einzuschüchtern und die Unbefangenheit des Kunden bei der Nutzung des Internets zu beeinträchtigen.[70] Die gegenwärtige Praxis ist somit rechtswidrig. Es ist davon auszugehen, dass ein Großteil der dynamischen IP-Adressen zu Unrecht erhoben, gespeichert und verwendet wird. Eine auf dynamische IP-Adressen beschränkte Vorratsdatenspeicherungsregelung im Sinne einer anlasslosen Erhebungs- und Speicherpflicht existiert nicht.

2.2.1.2 Voraussetzungen

§ 100g StPO legt die Voraussetzungen des Zugriffs auf Verkehrsdaten fest; der Gegenstand des Auskunftsverfahrens ergibt sich aus dem TKG. Die Konzeption entspricht damit der des Doppeltürmodells. Es reicht der Anfangsverdacht der Täterschaft oder Teilnahme an einer Tat i.S.d. § 100g StPO aus.[71] Eine Straftat von im Einzelfall erheblicher Bedeutung (§ 100g Abs. 1 S. 1 Nr. 1 StPO) oder eine mittels Kommunikation begangene Straftat (§ 100g Abs. 1 S.1 Nr. 2 StPO) ist Voraussetzung. Von erheblicher Bedeutung sind Straftaten, die dem Bereich der mittleren Kriminalität zuzuordnen sind, den Rechtsfrieden empfindlich

---

details0/artikel/vodafone-wehrt-mit-loschelder-unberechtigte-auskunftsersuchen-von-abmahnern-ab-datenschutz-im-inte.html.

[69] Eine enge Auslegung fasst unter Störungen nur solche, die in Zusammenhang mit der Übertragung der Nachricht stehen (anlassabhängig). Der Erforderlichkeitsgrundsatz führt damit erneut zu einer unverzüglichen Löschungspflicht gem. § 96 Abs. 1 S. 3, wenn kein Anlass vorliegt, vgl. *Braun* a.a.O. und *Breyer* MMR 2011, 573.

[70] Anders der *BGH* NJW 2011, 1509, 1512. Dort wo über die Speicherung zur Entgeltabrechnung angesichts von Flatrate-Tarifen überhaupt kein Raum bleibt, vermag (auch nach Rückschluss der Ansicht des *BGH*) nur noch § 100 TKG eine Erhebung rechtfertigen. Eine Verwendung für repressive Zwecke über § 100 TKG liegt nahe.

[71] *Schmitt,* in: *Meyer-Goßner*, StPO, 56. Aufl. 2013, § 100g, Rn. 14 i.V.m. § 100a, Rn. 9.

stören und geeignet sind, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen.[72] Hinzu treten durch die Rückverweise des § 100g Abs. 2 auf § 100b Abs. 1-4 StPO die verfahrenssichernden Elemente einer nachträglichen Benachrichtigungspflicht sowie ein vorgeschalteter Richtervorbehalt.

2.2.2 Die Vorratsdatenspeicherung: anlasslose Speicherung von Verkehrsdaten auf Vorrat

Nunmehr gibt es zwei maßgebliche Urteile, an denen sich eine zukünftige Umsetzung einer Vorratsdatenspeicherung in Deutschland (bzw. der EU) messen lassen muss.

2.2.2.1 Die Vorratsdatenspeicherung im Lichte der Rechtsprechung des BVerfG

Die Verfassungswidrigkeit der §§ 113a, 113b TKG und des § 100g StPO, soweit auf § 113a TKG verwiesen wird, gründet sich nicht darauf, dass eine vorübergehende begrenzte Speicherpflicht „schlechthin unvereinbar"[73] mit dem Grundgesetz ist, sondern darauf, dass einerseits die Datensicherheit durch § 113a TKG nicht ausreichend garantiert wird[74] und andererseits der Zugriff unter den Voraussetzungen der §§ 113b TKG i.V.m. 100g Abs. 1 S. 1 StPO auf diese Daten nicht den Grundrechtseingriff in das Telekommunikationsgeheimnis rechtfer-

[72] Vgl. BT-Drs. 16/5846 S. 40; *Schmitt*, in: *Meyer-Goßner* (Fn. 72), § 100g, Rn. 13. Mit der beispielhaften Nennung des § 100a StPO wird lediglich richtungsgebend darauf hingewiesen, dass schwere Straftaten in jedem Falle ausreichen.
[73] *BVerfG* NJW 2010, 833, 873.
[74] Der Verweis auf die Regelungen zu techn. Sicherheitsvorkehrungen (§ 109 TKG) reiche nicht aus. Die Konkretisierung bleibe den Unternehmen überlassen; ein ausgeglichenes Sanktionensystem fehle, vgl. Pressemitteilung des *BVerfG* Nr. 11/2010 vom 2. März 2010 (Nr. 5); *BVerfG*, 1 BvR 256/08, Urteil vom 2.3.2010, LS 1, Absatz-Nr. 221 ff. - vgl. auch *BVerfG* NJW 2010, 833, 840.

tigt[75]. Hier bemühte das BVerfG den Passus des „diffus bedrohliches Gefühl des Beobachtetseins“ durch eine anlasslose Speicherung von Verkehrsdaten.[76] Hierzu bedürfe es einen durch einzelne Tatsachen begründeten Verdacht einer allgemeinen und auch im Einzelfall schwerwiegenden Straftat, der Anlass für eine Erhebung der entsprechenden Daten gebe.[77]

2.2.2.2 Die Vorratsdatenspeicherung nach dem EuGH-Urteil 2014

Mit Urteil in den verbundenen Rechtssachen C-293/12 und C-594/12 vom 8.4.2014 hat der EuGH die Richtlinie zur Vorratsdatenspeicherung für ungültig erklärt.[78] Der EuGH sieht einen Eingriff in die Grundrechte auf Achtung des Privatlebens (Art. 7) und auf Schutz personenbezogener Daten (Art. 8) der Grundrechtecharta ebenfalls nicht ausreichend gerechtfertigt. Die Richtlinie sei unverhältnismäßig, da sie nicht zu gewährleisten vermöge, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränke.[79] Sie verpflichte zu einer unterschiedslosen Speicherung ohne Differenzierung nach Person, Kommunikationsmittel oder bestimmtem Verkehrsdatum.[80] Die Zugriffsvoraussetzung der „schweren Straftat“ reiche für eine notwenige Beschränkung des Zugriffs nicht aus.[81] Zuletzt sei auch eine unterschiedslose Speicherfrist ohne Unterscheidung nach Person, Nutzen und Ziel abzulehnen.[82]

---

[75] § 113b Satz 1 Nr. 2 und 3 TKG genüge den Anforderungen an eine hinreichende Begrenzung der Verwendungszwecke nicht. Die Bereitstellung eines offenen Datenpools hebe den notwendigen Zusammenhang zwischen Speicherung und Speicherungszweck auf, vgl. Angaben vorhergehende Fn.
[76] *BVerfG* NJW 2010, 833, 839.
[77] A.a.O., 840.
[78] Urteil ist abrufbar unter http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclanDE; a.a.O. Rn. 32 ff.
[79] A.a.O. Rn. 52 ff.
[80] A.a.O. Rn. 57
[81] A.a.O. Rn. 60 ff.
[82] A.a.O. Rn. 63 ff.

2.2.2.3 Ausblick

Es bleibt abzuwarten, ob die Vorratsdatenspeicherung weiter forciert wird. Letzteres ist nur schwer vorstellbar, scheint aber zumindest bis zur Einführung der europäischen Datenschutzgrundverordnung „auf Eis".[83] Allerdings ist es dem deutschen Gesetzgeber unbenommen, eine eigene verfassungsmäßige und europarechtskonforme Regelung zu schaffen.[84] Der deutsche Justizminister hat einer nationalen Regelung nach dem EuGH-Urteil zwar die Eilbedürftigkeit der Einführung mangels nunmehr fehlender Umsetzungspflicht abgesprochen, doch drängt die koalitionsvertragliche Vereinbarung, geschweige denn das Interesse der Strafverfolgungsbehörden, zu einer weitergehenden politischen Diskussion über die Umsetzung.

2.3 Inhaltsüberwachung

Der Zugriff auf Inhalte kann auf verschiedensten Wegen erfolgen: Beschlagnahme beim Nutzer, heimliche Beschlagnahme beim Provider, Abfangen von Daten oder auch Auslesen frei zugänglicher Informationen im Netz und sozialen Netzwerken. Je nach konkreter Ausgestaltung ändert sich die Intensität des Eingriffs bei dem Zugriff auf die Inhaltsdaten.

---

[83] So *Cecilia Malmström*, die ehemalige europäische Kommissarin für Justiz, vgl. http://www.heise.de/newsticker/meldung/EU-Kommission-unternimmt-keinen-neuen-Anlauf-zur-Vorratsdatenspeicherung-2215883.html. Die Pläne der neuen Kommission sind abzuwarten.

[84] Justizminister *Maas* will nicht ohne eine europäische Regelung tätig werden, vgl. http://www.heise.de/newsticker/meldung/Justizminister-Kein-nationaler-Alleingang-zur-Vorratsdatenspeicherung-2218482.html.

2.3.1 Online-Streife und Ausforschung sozialer Netzwerke

Die sog. Online- oder auch Internet-Streife ist mittlerweile hinlänglich bekannt. Eine weitere Spielart, die bedingt anders gelagert ist, ist die Ausforschung sozialer Netzwerke.

2.3.1.1 Ziel und Durchführung der Online-Streife

Mittels Online-Streife wird wortgetreu eine generalpräventive Aufgabe, die „Streifenfahrt im Internet", ausgeübt. Sie kann aber auch gezielt dazu dienen, Informationen über Personen zu erheben, zu sammeln und auszuwerten. Durch Polizeibeamte erfolgt eine Recherche in frei zugänglichen Online-Diensten. Dies sind vor allem das Internet und das Usenet mit seinen Newsgroups, Foren und Chaträumen.[85]

Erstere Variante ist als eine „anlassunabhängige Recherche in Datennetzen" zu klassifizieren und verdient daher den Namen „echte Online-Streife". Laienhaft handelt es sich schließlich um eine „digitale Präsenzaufgabe". Definitorisch ist es eine "ständige, systematische, deliktsübergreifende, nicht extern initiierte Suche nach strafbaren Inhalten im Internet und Online-Diensten".[86] Ein gezieltes Ermitteln hingegen ist eine „anlassbezogene Recherche in Datennetzen", nämlich „die durch anlassunabhängige Recherchen oder durch konkrete Hinweise und Anzeigen, aufgrund Ersuchen anderer Dienststellen oder als Ermitt-

[85] Vgl. http://www.bka.de/nn_206376/DE/DasBKA/Aufgaben/Zentralstellen/ZaRD/zard__node.html?__nnn=true. Die Beweiserhebung, -sicherung und -dokumentation, wie sie das BKA beschreibt, gehört hier nicht zu. Es kommt hierdurch zu einem Grundrechtseingriff. Dieser kann nicht durch die gewöhnliche Aufgabenwahrnehmung der Polizei gerechtfertigt werden, vgl. *BVerfGE* 120, 274, 345. Für das BKA spielt dies freilich keine Rolle, da eine eigens geschaffene Ermächtigungsgrundlage mit § 2 BKAG besteht.

[86] In Anlehnung an die Begriffsverwendung durch das BKA und modifiziert nach der hier vertretenen Auffassung, dass nur die anlassunabhängige Datenrecherche eine „echte Online Streife" darstellt, Vgl. http://www.bka.de/nn_206376/DE/DasBKA/Aufgaben/Zentralstellen/ZaRD/zard__node.html?__nnn=true.

lungen begleitende Maßnahme, zur Weiterverfolgung von festgestellten, strafrechtlich relevanten Sachverhalten sowie die Beweissicherung bis zur Feststellung der Verantwortlichen im Internet und Online-Diensten".[87] Es handelt sich um eine „unechte Online-Streife", da mit ihr nicht nur gestreift wird, sondern gezielt ermittelt. Die hier gewählten Bezeichnungen sind demnach vom Maßnahmezweck abhängig. Dies hat gleichsam Bedeutung für die Ermächtigungsgrundlagen der „Online-Streifen".

2.3.1.2 Rechtsgrundlage

Die echte Online-Streife benötigt keine Ermächtigungsgrundlage. Die vorgefundenen Informationen sind frei zugänglich. Es handelt sich um „allgemeine Aufklärung".[88] Es lässt sich vertreten, dass die bewusste Preisgabe durch die Internetnutzer sogar einen Grundrechtsverzicht darstellt.[89] In Kohärenz mit dem Urteil des BVerfG zur Online-Durchsuchung und der Rechtsprechung des BVerfG zur Wesentlichkeitstheorie liegt demnach kein Eingriff in Grundrechte vor, solange auf frei zugängliche Informationen zugegriffen wird, kein gezieltes Zusammentragen, Speichern und Auswerten erfolgt und kein schutzwürdiges Vertrauen der Teilnehmer einer Internetkommunikation verletzt wird.[90] Für die echte Online-Streife ist die polizeiliche Aufgabenbeschreibung mithin ausreichend – und zwar diejenige im präventiv polizeilichen Aufgabenbereich der Gefahrenabwehr und nicht derjenigen der Strafverfolgung. „Anlassunabhängig" bedeutet insofern „verdachtslos".

---

[87] Diese selbstformulierte Definition ist angelehnt an die Beschreibung der „anlassunabhängigen Recherche in Datennetzen" des BKA und wurde entsprechend der hier vertretenen Ansicht verändert.
[88] So auch *Keller* KR 2009, 491, 497.
[89] *Kudlich* GA 2011, 197, 199.
[90] *BVerfG* NJW 2008, 822, 835 f.

Bei der unechten Online-Streife ist dies anders.[91] Die Verdachtsbezogenheit („anlassbezogen") bedingt, dass gezielt Informationen zusammengetragen werden; es kommt zu Erhebung, Speicherung und Auswertung von Daten. Hierin liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung.[92] Die Ermittlungsgeneralklausel ist taugliche Rechtsgrundlage. Gleiches gilt bei der Straftatenvorsorge zur Prüfung des Anfangsverdachts.[93] Die §§ 161, 163 StPO reichen für diesen Fall unstreitig aus.[94]

2.3.1.3 Sonderfall: Ausforschung sozialer Netzwerke

Beim Zugriff auf soziale Netzwerke ist ausschlaggebend, ob durch die Nutzung eines Netzwerkes schutzwürdiges Vertrauen der Teilnehmer begründet wird. Ist dies der Fall, so reicht nicht mehr die Ermittlungsgeneralklausel aus. Es wird dann rechtlich kein „nicht offen ermittelnder Polizeibeamter (NoeP)" eingesetzt, sondern ein verdeckter Ermittler (es sind die höheren Anforderungen des § 110a StPO zu erfüllen).[95] Die konkreten Aktivitäten reichen von einer lediglich passiven Beobachtung der Teilnehmerinteraktion, wie das Verfolgen von „Pinnwand"-Einträgen bei Facebook oder eines Chatverlaufs, bis hin zur aktiven Kontaktaufnahme zu einem oder mehreren Nutzern. Allein durch die Zugangsbeschränkungen des Netzwerks kann schutzwürdiges Vertrauen in die Existenz

---

[91] Die unechte Online Streife. erfolgt hingegen auch durch Anmeldung in Chaträumen, sozialen Netzwerken oder Foren mit „Nicknames". Ebenso kann ein gezieltes Suchen nach Informationen eine Kontaktaufnahme mit Internetteilnehmern und eine länger andauernde Ermittlung notwendig machen.
[92] *BVerfGE* NJW 2008, 822, 836.
[93] *Griesbaum,* in: Karlsruher Kommentar StPO, 7. Aufl. 2013, § 161, Rn.1.
[94] Statt vieler *Keller* KR, 2009, 491, 497. Selbst wenn der Zugang beschränkt ist, bedarf es nicht sofort einer weitergehenden Ermächtigungsgrundlage. Ist eine Anmeldung nicht unter Klarnamen gefordert und unprüfbar, geht es nicht um tatsächliche Einschränkungen des Zugangs, sondern nur um die „personenspezifische Speicherung bestimmter Einstellungen", siehe *Kudlich*, GA 2011, 197, 199.
[95] Name, Anschrift, Beruf, Werdegang, Konfession, Nationalität, familiäre und sonstige Beziehungen, vgl. *Pegel,* in: *Radtke/Hohmann*, StPO-Kommentar, § 110, Rn. 4

und Vertrauenswürdigkeit der Teilnehmer bestehen (äußere Abgrenzungsmerkmale: z. B. Kreditkarteninformationen die durch den Host verifiziert werden, gleiches gilt auch für Jobbörsen wie Xing).[96] Ist dies der Fall, muss ein verdeckter Ermittler zum Einsatz kommen, ebenso bei einer länger andauernden aktiv-rezeptiven Teilnahme und einem Einwirken auf Nutzer zur Erlangung von Informationen (innere Abgrenzungsmerkmale).[97]

2.3.2 Die „gewöhnliche" Telekommunikationsüberwachung

Die Überwachung von Telekommunikation ohne Wissen des Betroffenen ist technisch und rechtlich möglich. Rechtsgrundlage für die Telekommunikationsüberwachung (TKÜ) ist § 100a StPO.

2.3.2.1 Ziel und Anwendungsbeispiele

Der § 100a StPO ist eine verdeckte Überwachungsmaßnahme. Der Zugriff nach § 100a StPO erfolgt netzgebunden durch Eingriff in den technischen Vorgang des Übertragens der Signale. Die Telekommunikationsunternehmen sind hierbei notwendige Kooperationspartner.[98] Die Heimlichkeit ist der Überwachung

---

[96] Vgl. auch die Antwort auf eine kleine Anfrage zur Nutzung sozialer Netzwerke durch „virtuelle Ermittler", BT-Drs. 17/6587, S. 3. Da soziale Netzwerke in der Regel eine vorherige Anmeldung und einen mehr oder weniger umfangreichen Registrierungsprozess erfordern, muss sich der Ermittlungsbeamte Zugang mittels falscher persönlicher Angaben verschaffen. Dies sind beispielsweise erdachte Klarnamen, Nicknames oder eigens hierfür erstellte E-Mailadressen. Es können je nach Dienst weitere Angaben erforderlich sein, z. B. Angaben über Beruf, Familienstand, Wohnort etc. bis hin zu einem Online-Auftritt unter vollständiger Legende.

[97] Eingehend *Rosengarten/Römer* NJW 2012, 1764 und *Henrichs/Wilhelm* KR 2010, 30. Eine trennscharfe Abgrenzung ist demnach sehr schwierig und hängt vom Einzelfall der Ausgestaltung des jeweiligen Netzwerkes wie auch von dem Verhalten des Polizeibeamten ab.

[98] Sie sind gem. § 100b Abs. 3 StPO i.V.m. § 110 TKG und der Telekommunikationsüberwachungsverordnung verpflichtet, die Überwachung zu ermöglichen und Auskünfte zu erteilen. Sie haben auf eigene Kosten technische Einrichtungen zur Umsetzung von Überwachungsmaßnahmen vorzuhalten (§ 110 Abs. 1

immanent, andernfalls könnten Gegenmaßnahmen getroffen oder die Kommunikation gestoppt werden.[99] Hieraus resultiert ihre hohe Eingriffsintensität, die mit hohen Eingriffsvoraussetzungen korreliert. Erfasst werden alle Arten der Telekommunikation: E-Mail-Abfrage, Up- und Download via FTP-Server, VoIP etc.

Ungeklärt ist, ob der § 100a StPO auf rein technische Telekommunikationsvorgänge anwendbar ist, die keinen gedanklichen Austausch zwischen zwei oder mehr individualisierbaren Personen zum Gegenstand haben. M.E. darf sich die Anwendung nur auf solche Inhalte beziehen, die auch durch Art. 10 GG geschützt werden (Inhaltslösung). Solche Inhalte die notwendigerweise über die Internetverbindung transportiert werden, z. B. die Daten, die für die Cloud bestimmt sind oder Daten die beim „rumsurfen" ausgetauscht werden, fallen heraus.[100] § 100a StPO erfasst also nicht alle durch Dienstanbieter vermittelte Vorgänge unabhängig von den Beteiligten.[101]

2.3.2.2 Voraussetzungen

Die Überwachung kann sowohl beim Beschuldigten, wie auch beim sog. Nachrichtenmittler erfolgen (§ 100a Abs. 3 StPO). Der Adressat muss durch einen hinreichend konkreten Tatverdacht identifizierbar sein (arg. ex. § 100b Abs. 2 Nr. 1 StPO). Hierzu müssen gem. § 100a Abs. 1 Nr. 1 StPO bestimmte Tatsachen

---

Nr. 1 TKG). Die Maximaldauer der Anordnung beträgt drei Monate (Verlängerung um drei Monate nach erneuter Prüfung möglich).

[99] Z. B. Verschlüsselung der Kommunikation durch VPN oder https-Verbindung, oder Umleitung über Server im Ausland.

[100] Hierzu gehört die allgemeine „Kommunikation mit dem Internet", bspw. auch die Online-Erstellung persönlicher Inhalte wie Text- oder Fotobearbeitung, die nicht Teil von Individualkommunikation sind und auch nicht werden sollen.

[101] A.A. wohl *Bär*, der dies unter dem Stichwort „Kommunikationslösung" zusammenfasst (MMR 2013, 700, 703), wonach bereits das Vorliegen eines technischen Kommunikationsvorgangs § 100a StPO anwendbar macht. Als Pendant und in Anlehnung fungiert die hier vertretene „Inhaltslösung". Dies hat zur Folge, dass etwa rein privat genutzte Cloud-Speicher nicht über § 100a StPO ausgeforscht werden dürfen oder in die Datenverbindung interveniert werden darf.

den Verdacht begründen, dass jemand Beteiligter einer schweren Straftat aus dem Katalog des § 100a Abs. 2 StPO ist. Ein „einfacher" Tatverdacht, also Tatsachen die nach der Lebenserfahrung mit erheblicher Wahrscheinlichkeit darauf hindeuten, dass jemand Beteiligter einer Katalogtat ist, reicht erneut aus.[102] „Schwere Straftaten" sind solche, die „eine Mindesthöchststrafe von fünf Jahren Freiheitsstrafe aufweisen, in Einzelfällen aufgrund der besonderen Bedeutung des geschützten Rechtsguts oder des besonderen öffentlichen Interesses an der Strafverfolgung aber auch eine geringere Freiheitsstrafe."[103] Die Telekommunikationsüberwachung muss gem. § 100a Abs.1 Nr. 3 StPO ultima ratio sein.[104] Zum einen kommt die Telekommunikationsüberwachung nicht in Betracht, wenn andere Maßnahmen erfolgversprechend(er) sind (Subsidiarität), zum anderen gilt der allgemeine Verhältnismäßigkeitsgrundsatz nach Ausmaß des Eingriffs, Erfolgsaussichten und Grad des Tatverdachts.[105] Allerdings gilt für die Strafverfolgung im Internet oftmals, dass aufgrund der Datenflüchtigkeit und Datenubiquität bei weltweiter Vernetzung, kein gleich wirksameres, milderes

---

[102] *Roggan,* in: *Roggan/Kutscha*, Handbuch zum Recht der inneren Sicherheit, 2. Aufl. 2006, S. 110 (mit Bezug zu § 100c StPO, der den gleichen Verdachtsgrad erfordert). Der Tatverdacht muss ein gewisses Maß an Konkretisierung erreichen und von erheblicher Stärke sein, vage Anhaltspunkte und bloße Vermutungen (bspw. aus kriminalistischer Erfahrung oder auf Basis von Gerüchten) sind nicht ausreichend, vgl. *Schmitt,* in: *Meyer-Goßner* (Fn. 72), § 100a, Rn. 9; *Bär*, TK-Überwachung, § 100a, Rn. 17, *Röwer,* in: *Radtke/Hohmann* (Fn. 96), § 100a, Rn. 10.

[103] Vgl. BT-Drs. 16/5846, S. 40. Die „schwere Straftat" ist zwischen der „besonders schweren Straftat" (§ 100c StPO) und „Straftat von erheblicher Bedeutung" (§ 100g StPO) anzusiedeln (vgl. BT-Drs. 16/5846, S. 40). Da die Straftat jedoch auch im Einzelfall schwer wiegen muss (§ 100a Abs. 1 Nr. 2 StPO), gewinnt das Merkmal über den rein deklaratorischen Charakter hinaus an Bedeutung - etwa für eine Straftat nach § 86 StGB deren Strafandrohung maximal drei Jahre beträgt, siehe BT-Drs. 16/6979, S. 43.

[104] D.h. die Ermittlungen müssten ohne die Durchführung aussichtslos sein oder zumindest erschwert werden.

[105] *Röwer,* in: *Radtke/Hohmann* (Fn. 96), § 100a, Rn. 13. Vor allem die Qualität der Informationen die über eine Telekommunikationsüberwachung erlangt werden können, wie auch die Möglichkeit einer längeren heimlichen Ermittlung im Gegensatz zum Sofortzugriff spielen eine Rolle bei der Abwägung.

Mittel (z. B. Durchsuchung, Beschlagnahme) vorliegt. In solchen Fällen kommt nur eine Maßnahme nach § 100a StPO in Betracht.[106]

Hinzu treten, wie auch schon bei der Verkehrsdatenabfrage, verfahrenssichernde Elemente. Die formellen Verfahrensvoraussetzungen ergeben sich aus § 100b StPO. Wichtig ist, neben der Benachrichtigungspflicht des Betroffenen samt Rechtsmittelbelehrung (§ 101 Abs. 4 StPO), die Abfederung des intensiven Grundrechtseingriffs durch vorsorglichen Rechtsschutz im Rahmen des Richtervorbehalts gem. § 100b Abs. 1 StPO. Es besteht zudem Kontrolle durch die Berichtspflicht der Länder gegenüber dem Bundesamt der Justiz gem. § 100b Abs. 5 StPO. Inhalte, die dem Kernbereich der persönlichen Lebensgestaltung zuzuordnen sind, sind zu löschen gem. § 100a Abs. 4 StPO.

2.3.2.3 Exkurs: Zugriff auf E-Mails

Der heimliche Zugriff hat sich an § 100a StPO zu orientieren. Dies gilt unstreitig für die E-Mail, die gesendet und sodann abgefangen wird. Es muss m.E. aber gleichermaßen für eine Beschlagnahme der Mail auf dem Server des Providers gelten. § 100a StPO ist in seiner Ausformung schließlich für heimliche Maßnahmen konzipiert. Es kommt insofern nicht darauf an, dass es sich bei einem Zugriff auf die „ruhende Mail" beim Provider nicht um einen Eingriff in einen dynamischen Telekommunikationsvorgang handelt. Ein Eingriff in Art. 10 GG liegt jedenfalls vor.[107] Ausschlaggebend ist die mangelnde Beherrschbarkeit der eigenen Daten des Nutzers. Diese verdienen einen höheren Schutz als den der Beschlagnahmevorschriften der §§ 94 ff. StPO.[108] Konsequent wäre es also den § 100a StPO auf statische Telekommunikationsvorgänge auszudehnen.

---

[106] *Bär*, TK-Überwachung, § 100a, Rn. 24
[107] *BVerfGE* 124, 43, 53-58 - Erwägungsgründe I. und II
[108] So auch *Klein* NJW 2009, 2996, 2998, vgl. auch *Krüger*, *BVerfG* MMR 2009, 673, 683, *Singelnstein* NStZ 2012, 593, 596 f.

Auch § 99 StPO in entsprechender Anwendung der Maßnahmen zur Postbeschlagnahme ist nicht ausreichend.[109] Für § 99 StPO spricht zwar, dass er speziell auf den heimlichen Zugriff zugeschnitten ist, er gilt aber nur für Postbrief und Telegramm.[110] Das BVerfG fordert für den heimlichen Zugriff aufgrund der Schwere des Eingriffs aber „besonders hohe Anforderungen an die Bedeutung der zu verfolgenden Straftat und den für den Zugriff erforderlichen Grad des Tatverdachts".[111] Diesen Anforderungen wird § 99 StPO nicht gerecht. Das BVerfG hebt die Anforderungen für einen Zugriff auf ruhende Mails mindestens auf die des § 100g StPO.[112] Damit geht die Rechtsprechung des BGH zur Anwendung des § 99 StPO für heimliche Zugriffe auf E-Mails fehl.[113] Der Umstand, dass der § 100g StPO bereits erhöhte Anforderungen an die Bedeutung der Straftat stellt, obwohl es „nur" um Verkehrsdaten geht, lässt gegenwärtig nur einen Schluss zu: § 100a StPO eignet sich „am ehesten", den verfassungsrechtlichen Anforderungen an den heimlichen Zugriff auf E-Mails beim Provider gerecht zu werden. § 100a StPO ist somit auch auf statische Telekommunikationsvorgänge anzuwenden, sofern auf Inhaltsdaten eines Individualkommunikationsvorgangs zwischen mindestens zwei Personen zugegriffen wird. Dieser Schluss vereint die technikoffene Gestaltung des § 100a StPO mit der des Art. 10 GG. Beide Normen umfassen so übereinstimmend die „Stop-Forward-Kommunikation" des E-Mail-Verkehrs.

De lege ferenda ist es dennoch erforderlich, dass eine spezielle Eingriffsermächtigung zur heimlichen Beschlagnahme von E-Mails geschaffen wird, etwa eine Norm auf Niveau des § 100g StPO, die Straftaten erheblicher Bedeutung um-

---

[109] A.A. *Graf*, in: Beck-OK StPO, § 100a, Rn. 30. § 99 StPO wird in der Praxis herangezogen. Die Voraussetzungen liegen deutlich unter denen des § 100a StPO.

[110] Der *BGH* erweitert dies aufgrund der Kommunikationsangewohnheiten lapidar auf E-Mails, vgl. *BGH* NJW 2009, 1828

[111] *BVerfGE* 124, 43, 63.

[112] So auch *Klein* NJW 2009, 2996, 2999.

[113] A.A. *Graf*, Beck-OK StPO, § 100a, Rn. 30.

fasst und zusätzlich bestimmte internetspezifische Straftaten in einen Katalog aufnimmt. Eine fehlende Kohärenz zwischen Verkehrsdaten und Inhaltsdaten steht nicht entgegen, denn auch ein massenhafter Verkehrsdatenzugriff lässt Rückschluss auf rezipierte Inhalte zu und vermag Einblicke in den Kernbereich der privaten Lebensgestaltung ermöglichen. Der augenfällige Unterschied des § 100g StPO zu einer E-Mail-Zugriffsnorm auf Niveau des § 100g StPO wäre somit nur ein begrifflicher.

2.3.3 Quellen-TKÜ

Über die Zulässigkeit der Quellen-TKÜ nach gegenwärtigen Rechtsgrundlagen wird lebhaft gestritten.[114] Fest steht, dass derzeit keine repressive Ausübung erfolgt.

2.3.3.1 Ziel und Durchführung

Bei der Quellen-TKÜ handelt es sich um die Infiltration des Computers durch (fern-)installierte Software zum Abfangen und Ausleiten von Kommunikationsdaten zum Zeitpunkt des Aussendens. Ziel ist, die Inhalte einer Telekommunikationsverbindung abzufangen noch bevor diese verschlüsselt werden.[115] Viele Verschlüsselungsprogramme sind nämlich nicht oder nicht zeitnah dekryptierbar.[116] Die Überwachung wird zeitlich und räumlich an die Quelle vorverlegt.

---

[114] Für eine Quellen-TKÜ: *LG Hamburg* MMR 2011, 693; *LG Landshut* NStZ 2011, 479; *AG Bayreuth* MMR 2010, 266; *Bär*, TK-Überwachung, § 100a, Rn. 32 f.; *Schmitt* in *Meyer-Goßner* (Fn. 72), § 100a, Rn. 7a; *Nack,* in: KK-StPO, § 100a, Rn. 27f. ; *Graf,* in: BeckOK-StPO, § 100a, Rn. 107c ff.; *Stadler* MMR 2012, 18, 19. Dagegen: *LG Hamburg* MMR 2008, 423; *Sankol* CR 2008, 13, 15); *Becker/Meinicke*, StV 2011, 50, 52); insbesondere auch der Generalbundesanwalt in einer Stellungnahme vom 29.10.2010 zur Anwendung der Quellen-TKÜ bei einem Verfahren des *BGH*, abrufbar unter https://fragdenstaat.de/files/foi/7011/Gutachten_Quellen_TK.pdf.

[115] Auch bei einer Umleitung des Internetverkehrs über Proxykaskaden würde eine Quellen-TKÜ eventuelle Probleme bei Rechthilfefragen von vornherein verhindern.

[116] *Graf,* in: Beck-OK StPO, § 100a, Rn. 107a.

Ein Zugriff auf Festplatteninhalte ist (konzeptionell) nicht das Ziel. Die Quellen-TKÜ ist damit technisches Minus zur Online-Durchsuchung. Eine Software (bspw. Digitask oder FinSpy/Finfinisher) wird über eine Internetverbindung „virusgleich" auf das Endgerät des Betroffenen gespielt.[117] Sie ermöglicht bei Eingabe des Kommunikationsinhalts, sei es durch Registrierung des Tastendrucks (sog. Keylogger) oder Aktivität des Mikrofons zur Internettelefonie, die Überwachung.

2.3.3.2 De lege lata zulässig?

Nach zutreffender Ansicht rechtfertigt § 100a StPO eine Quellen-TKÜ. Das „rechtliche" Problem bei der Suche nach einer existierenden Rechtsgrundlage findet seinen Ursprung im Urteil des BVerfG zur Online-Durchsuchung.

Das Gericht statuiert hierin die Zulässigkeit einer Quellen-TKÜ, sofern der Zugriff ausschließlich auf einen laufenden Datenstrom durch „technische Vorkehrungen und rechtliche Vorgaben" sichergestellt sei.[118] Daraus wird abgeleitet, dass das BVerfG die gegenwärtigen rechtlichen Vorgaben nicht für ausreichend erachtete.[119] Dem ist zu widersprechen. Zum einen ging es bei der Entscheidung nicht um repressive Normen, zum anderen nicht einmal um die Quellen-TKÜ. Das Gericht tätigt auch nicht die Aussage, dass mit einer Infiltration eines informationstechnischen Systems ein schwerwiegenderer Eingriff vorliegt als bei der netzgebundenen Telekommunikationsüberwachung. Es wies nur darauf hin, dass hierdurch die entscheidende Hürde zur Ausspähung des Systems genommen sein „kann", nämlich dann, wenn technische Vorkehrungen der Spähsoftware dies nicht verhindern. Weiter noch stellt das BVerfG sogar fest, dass die Quellen-TKÜ ausschließlich an Art. 10 GG zu messen sei, sofern

[117] BKA/Zoll haben in 21 Verfahren 2007-2011 eingesetzt - v.a. BTM, Terrorismus u. Geldwäsche (BT-Drs. 17/7760, S. 11 ff.)
[118] *BVerfGE* 120, 274, 309.
[119] So etwa die Ansicht des Generalbundesanwalts in seinem Gutachten.

sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränke. Eingedenk ausreichender technischer Vorkehrungen ist damit die Infiltration des Systems unter Eingriff in Art. 10 GG sehr wohl gerechtfertigt. § 100a StPO ist hierfür die richtige Norm.

Technisch ist ein Instrument nötig, dass das Spezialitätsverhältnis der Grundrechte (Telekommunikationsgeheimnis vs. IT-Grundrecht) umsetzt, also ein solches, dass ein Auslesen des Datenbestandes des informationstechnischen Systems nicht zulässt, sondern nur den Zugriff auf einen konkreten dynamischen Telekommunikationsvorgang. Eine Annexkompetenz zur Infiltration ist als sekundäre Vorbereitungs- und Begleitmaßnahme regelmäßig durch die Primärbefugnis gedeckt.[120] Eine leitungsbezogene Begrenzung der Überwachung ergibt sich aus § 100a StPO nicht, sodass auch das Endgerät technischer Anknüpfungspunkt sein kann.[121] „Typischerweise" ist die Quellen-TKÜ mithin die einzig wirkungsvolle Maßnahme zur Überwachung bei kryptierten Signalen.[122]

Dennoch wäre eine Klarstellung in der StPO bedenkenswert und schnell umsetzbar. Die Einfügung eines Unterabsatzes könnte rein deklaratorisch bestim-

---

[120] *Bär*, TK-Überwachung, § 100a, Rn. 32 f., *Graf*, in: Beck-OK StPO, § 100a, Rn. 107f.; a.A. *AG Hamburg,* Urt. v. 28.08.2009, Az.: 160 Gs 301/09 abrufbar unter http://www.ja-aktuell.de/root/img/pool/urteile_im_volltext/4-2010/160_gs_301-09.pdf.

[121] Vgl. auch § 100b Abs.2 Nr.2 StPO in dem das zu überwachende „Endgerät" sogar namentlich Eingang findet. Die Gegenansicht lässt außer Acht, dass eine sinnvolle teleologische Auslegung der begriffsoffenen Anwendung des § 100a StPO nur möglich ist, wenn auch technische Sekundärmaßnahmen begriffsoffen einbeziehbar sind, zumal die „ferngesteuerte" Infiltration des Systems unter Verhältnismäßigkeitsgesichtspunkten das geeignetste und mildeste Mittel ist.

[122] Das *AG Hamburg* verneint auch eine Vergleichbarkeit mit § 100f StPO und dem typischerweise erfolgenden Öffnen des PKW zur Anbringung von Überwachungstechnik. Es verkennt, dass bei der zur Überwachung kryptierter Nachrichten „typischerweise" zu einer Infiltration der Quelle kommen muss und es eben nicht „vielfältige" Überwachungsformen in einem solchen Falle gibt.

men, dass die TKÜ nach § 100a StPO auch in der Weise erfolgen kann, dass mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingegriffen werden darf, wenn durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.[123]

Legt man den § 100a StPO in der hier vertretenen Weise aus, dass nur Inhalte i.S.d. Art. 10 GG erfasst werden („Inhaltslösung"), so darf die Quellen-TKÜ eigentlich nicht zu einem Zugriff auf alle Daten eines Datenstroms führen. Der Festplattenschutz durch das IT-Grundrecht muss sich nämlich in der Datenkommunikation fortsetzen. Er erstreckt sich auf Inhalte, die Teil des Datenstroms sind, aber nicht den Schutz von Art. 10 GG genießen. Die Inhaltslösung schlägt sich damit als zweites Schutz- und Umsetzungskriterium für eine zulässige Quellen-TKÜ nieder. Die Software sollte neben dem „Muss" des Schutzes des IT-Systems im Idealfall bereits den Zugriff auf Inhaltsdaten eines Datenstroms, die nie für zwischenmenschliche Kommunikation i.S.d. Art. 10 GG bestimmt waren, verhindern. Da der isolierte Rohdatenzugriffs technisch aber (gegenwärtig) nicht umsetzbar ist, ist eine Gesamtbeurteilung des Nutzungsverhaltens des Maßnahmeadressaten im Rahmen des § 100a Abs. 4 StPO vorzunehmen. Der Kernbereichsschutz ist auf der Verwertungsebene durchzusetzen. Eine Quellen-TKÜ darf nicht durchgeführt werden, wenn tatsächliche Anhaltspunkte vorliegen, dass hierdurch allein oder weit überwiegend Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden (Erhebungsverbot). Bei einem Überwiegen der Telekommunikationsinhalte bestehen hingegen (nur) ein Verwertungsverbot und ein Löschungsgebot. Der

[123] Vgl. den Wortlaut der genannten präventiv-polizeilichen Vorschriften. Den vom Gericht geforderten, ex-ante Schutzmechanismus für den Kernbereich der privaten Lebensgestaltung durch Richtervorbehalt trägt § 100a StPO bereits durch Verweis des § 100b Abs. 1 StPO.

überschießende Anteil der Datenkommunikation, der nicht Telekommunikationsbestandteil i.S.d. Art. 10 GG ist, ist zu löschen.

2.3.4 Online-Durchsuchung

Eine Online-Durchsuchung ist die Suche nach Inhaltsdaten durch den Zugriff auf Festplatteninhalte eines Computers mittels einer (fern-)installierten Software (im Popularwortschatz „Trojaner" genannt).[124] Der Zugriff erfolgt „von außen" unter Nutzung einer bestehenden Internetverbindung zur Übermittlung der Inhalte an die Strafverfolgungsbehörden.[125]

Anders als bei der Quellen-TKÜ ist Ziel nicht die Datenverbindung, sondern der Computer selbst. Teilweise wurden § 100a StPO oder § 102 StPO dennoch als ausreichende Eingriffsgrundlage angesehen.[126] Das BVerfG hat in seinem Urteil vom 27.02.2008 den präventiven Eingriffsgrundlagen in NRW die Verfassungsmäßigkeit abgesprochen und gleichzeitig die Maßstäbe für eine strafprozessuale Norm umrissen.[127] Diese müsse einen Eingriff in den Schutzbereich des IT-Grundrechts rechtfertigen.[128] In der Infiltration eines informationstechnischen Systems liege eine Gefährdung, die weit über die einer Telekommunikations-

---

[124] Das BKA entwickelte eine Remote Forensic Software (RFS) für Zwecke des verdeckten Eingriffs in informationstechnische Systeme , es kam zum Einsatz in mind. 7 Fällen (BT- Drcks. 17/7760, S. 10 - Beachte: NICHT repressiv)

[125] *Röwer,* in: *Radtke/Hohmann* (Fn. 96), § 100a, Rn. 19. Eine Infiltration des Wohnraums (Art. 13 GG) kann ausgeklammert werden, da es in der Diskussion um Softwarelösungen geht, die durch Ferninstallation ausgeführt werden (BT-Drs. 17/7760, Auskunft über Einsatz staatlicher Schadprogramme zur Computerspionage („Staatstrojaner"), Frage 28).

[126] *BGH*-Ermittlungsrichter für § 100a StPO*, BGH* NJW 1997*, 1934; Hofmann*, NStZ 2005, 121, 123ff.) für § 102 StPO. Ebenso auch von der Generalbundesanwaltschaft angenommen. Diese hatte beim Ermittlungsrichter des *BGH* beantragt, auf der Grundlage der §§ 102, 105 Absatz 1, 94, 98 StPO eine Online-Durchsuchung zu gestatten. Dies wurde abgelehnt; vgl. *BGH* MMR 2007, 174. Der Grund liegt im Zweck und den Möglichkeiten der Maßnahme.

[127] *BVerfGE* 120, 274, 302 ff.

[128] *BVerfGE* 120, 274.

überwachung hinausgehe.[129] Dies trifft zweifelsohne zu. Tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut (z. B. Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt), ein Richtervorbehalt sowie Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung müssen daher den Zugriff rechtfertigen.[130] Präventiv-polizeiliche Rechtsgrundlagen wurden seitdem geschaffen.[131] An einer strafprozessualen Norm oder Initiative fehlt es.

§ 100a StPO deckt die Online-Durchsuchung schon begrifflich nicht, da Ermittlungsziel nicht lediglich Telekommunikationsinhalte sind (respektive solche Daten, die es noch werden sollen) sondern Inhaltsdaten insgesamt. § 100a StPO rechtfertigt somit keinen Eingriff in das IT-Grundrecht. Die Begrenzung innerhalb des § 100a StPO auf schwere Straftaten wird einem unterschiedslosen Zugriff auf Inhalte, die (noch) nicht Telekommunikationsinhalt geworden sind und auch gar nicht werden sollen, nicht gerecht.[132] Die Regelung des § 100a Abs. 4 StPO weist zwar einen Schutzmechanismus zum Schutze des Kernbereichs privater Lebensgestaltung auf, doch dieser berücksichtigt nur Kommunikationsinhalte. Inhalte, die auf einer Festplatte auffindbar sind und weder aus einer Kommunikationsbeziehung herrühren, noch für eine solche bestimmt sind, weisen hingegen einen weitergehenden Kernbereichsbezug auf. Gleiches gilt für § 102 StPO. Er ermöglicht eine offene Ermittlungsmaßnahme und ist

[129] *BVerfGE* 120, 274, 308.
[130] A.a.O., 328 ff.
[131] § 20k BKAG, Art. 34d Bay PAG.
[132] Der Unterschied zu Inhalten, die etwa in eine Eingabemaske beim Web-Mail erstellt werden oder im Entwurfsordner gespeichert sind, ist derjenige, dass eine Konnexität in zeitlicher wie thematischer Hinsicht zu Individualkommunikation als Voraussetzung einer Anwendung des § 100a StPO nicht auf der Hand liegt, schwerlich festzustellen ist und diese Inhalte letztlich nicht einmal Ziel der Maßnahme sind.

nicht auf eine heimliche Infiltration und anschließende Durchsuchung zugeschnitten.[133]

Problematisch ist, dass das BVerfG (verständlicherweise) die Hürden für eine repressive Online-Durchsuchung derart hoch gehängt hat, dass sie im Wege nachvollziehender Gesetzgebung kaum umsetzbar erscheint. Vergegenwärtigt man sich die tatbestandlichen Voraussetzungen des § 100c StPO, der eine akustische Wohnraumüberwachung an das Vorliegen besonders schwerer Straftaten, einen Richtervorbehalt und einen weiten Kernbereichsschutz knüpft, um den Eingriff in Art. 13 GG zu rechtfertigen, so bleibt kein Spielraum mehr für eine Umsetzung der Online-Durchsuchung. Dies muss jedenfalls gelten, wenn man dem IT-Grundrecht in Schutzzweck und Kernbereichsbezug einen noch höheren Wert als Art. 13 GG beimisst. Das ist der Fall. Schließlich ist Ziel einer Maßnahme nach § 100c StPO, dass das gesprochene Wort abgehört wird, also letztendlich Kommunikation zwischen Personen, die einen besonderen Schutz im Wohnraum erfährt. Dieser Umstand schwächt den Kernbereichsbezug etwas ab, da die Inhalte nicht nur interner Natur sind, sondern nach dem Willen des Betroffenen nach außen kommuniziert werden. Anders bei einer Infiltration eines IT-Systems: Der Betroffene gibt hierbei zu keinem Zeitpunkt zu erkennen, dass irgendein Mensch auf der Welt etwas von den Dingen erfahren soll, die er auf seinem Gerät speichert. Entspricht dem Wohnraumelement bei § 100c StPO zwar die Infiltration der Festplatte, fehlt die Vergleichbarkeit spätestens beim Kommunikationselement. Wie eine Norm noch über dem Niveau des § 100c StPO in das Gefüge der telekommunikationsbezogenen Ermittlungsmaßnahmen eingebracht werden soll, bleibt ein Rätsel.

[133] *BGHSt* 51, 211, 212, Rn. 5; 215, Rn. 10.

3 Fazit

Handelt es sich denn nun um eine Mär? Ist der deutsche Staat ein „Überwachungsstaat“?

Der Gesetzgeber und die Ermittlungsbehörden haben sich neuen Herausforderungen angepasst. Es verbleiben bei den einzelnen vorgestellten Ermittlungsmaßnahmen dennoch Unsicherheiten und Unwägbarkeiten. Teils hängen diese mit unterschiedlichen Rechtsauffassungen zusammen, teils resultieren sie aus den technischen Rahmenbedingungen. Beste Beispiele hierfür sind die Vorratsdatenspeicherung und die Quellen-TKÜ. Das BVerfG monierte bei ersterer nicht umsonst, dass eine rechtmäßige Speicherung von Verkehrsdaten auf Vorrat v.a. auch an technischen Vorkehrungen zur Datensicherheit scheitert. Bei der Quellen-TKÜ krankt eine Anwendung an dem Einsatz einer Software, die tatsächlich nicht mehr „kann“, als nur Telekommunikation zu überwachen. Auf rechtlicher Seite zeigen bereits die hier vertretenen Ansichten, etwa zur Quellen-TKÜ, der E-Mail-Beschlagnahme oder die Modifikation des § 100a StPO durch die Inhaltslösung, dass es unzählige Meinungen und Gegenmeinungen gibt und geben wird. Der Streit über die Speicherberechtigung dynamischer IP-Adressen verdeutlicht die Konfusion ebenfalls gut: Warum regelt der Gesetzgeber die Abfrage dynamischer IP-Adressen, wenn diese durch die Diensteanbieter gar nicht rechtmäßig gespeichert werden dürfen?

Dieses Beispiel verstärkt einen interessanten, aber nicht minder erschreckenden Gedanken: Lässt der Gesetzgeber sich durch Strafverfolgungsinteressen leiten, ohne tatsächlich die notwendigen Voraussetzungen für eine rechtmäßige, grundrechtskonforme Anwendung geschaffen zu haben? Ein Schelm, wer ein System dahinter vermutet.

Viele Gesetze tragen in sich Unstimmigkeiten, die gerade aus einer Unklarheit über die Vorzeichen der Umsetzbarkeit resultieren. Dies gilt, um einige Beispiele zu nennen, m.E. für die Zuordnung dynamischer IP-Adressen, die Anwendung des § 113 TKG auf Clouds, die Aufnahme von Cloud-Zugangssicherungsdaten[134] sowie die Anwendung von § 110 Abs. 3 StPO auf Daten im Ausland.[135]

Indes ist der Gesetzgeber sehr wohl darauf bedacht Grundrechtseingriffen Rechnung zu tragen und verschließt sich hierbei nicht rechtswissenschaftlichen Argumenten.[136] Die kommunikationsbezogenen Ermittlungsmaßnahmen sind in ihren Voraussetzungen mit vorgreifenden und nachwirkenden rechtssichernden Verfahrenselementen ausgestaltet: Benachrichtigungspflichten, Richtervorbehalte, Berichts- und Dokumentationspflichten sowie Löschpflichten. Der deutsche Staat ist also kein Überwachungsstaat, sondern vielmehr ein Staat mit der „Befähigung zu einer (grundrechtskonformen) Überwachung."

Zu Recht jedoch wurde im Zuge der Telemedicus-Konferenz aus dem Plenum darauf hingewiesen, dass dies nur „Grundrechtsschutz auf dem Papier" sei. Ohne die praktische Umsetzung der erwähnten verfahrenssichernden Elemente

---

[134] Diese dürfen schließlich nur abgefragt werden, wenn die Voraussetzungen der Nutzung vorliegen. Ob es eine Rechtgrundlage gibt, die den Zugriff auf eine Cloud regelt, ist aber überhaupt nicht in die Erwägungen eingestellt worden. Eine offene Beschlagnahme ist nach §§ 94 ff. StPO möglich. Eine heimliche Beschlagnahme hingegen nicht. Eine Cloud ist kein Individualkommunikationsmittel. § 100a StPO scheidet in der Regel aus. In der Cloud als ausgelagerte Festplatte setzt sich vielmehr der Schutz der heimischen Festplatte fort. Dies bedeutet, dass an einen Cloud-Zugriff dieselben Voraussetzungen zu knüpfen sind wie an eine Online-Durchsuchung. De facto ist ein Zugriff also nicht möglich, der Zugriff auf die Zugangsdaten somit auch sinnlos und nicht durchführbar.

[135] Als Umsetzung des Art. 19 Abs. 2 Cybercrime-Konvention muss ein Zugriff sich auf das eigene Hoheitsgebiet beschränken, dies geschieht in der Praxis nicht.

[136] So etwa geschehen bei der Novelle des § 113 TKG und Schaffung des § 100j StPO. Ursprünglich war ein Richtervorbehalt für Zugangssicherungsdaten nicht geplant, Nach Anhörung verschiedener Rechtsexperten im BT wurde dieser aufgenommen. Prof. *Kugelmann* und Peter *Schaar* regten dies an.

gänzlich zu geißeln, muss diese Kritik als berechtigt gelten. Es bestehen „bei beiden Instrumenten (Benachrichtigung und Richtervorbehalt) erhebliche Bedenken hinsichtlich ihrer Tauglichkeit und ihrer Wirksamkeit“.[137] Der Beurteilungsspielraum des für die richterliche Anordnung zuständigen Ermittlungsrichters ist nur begrenzt überprüfbar, eine unabhängige Grenzziehung ist nicht möglich.[138] Hinzu kommt eine oftmals hohe Arbeitsbelastung. Mitteilungspflichten an den Beschuldigten nach Durchführung heimlicher Maßnahmen dürfen nicht unterlassen oder einfach „vergessen“ werden. Der Betroffene wird so seiner nachträglichen Rechtsschutzmöglichkeit beraubt.

Diese Kritik ist, wie eingangs erwähnt, ernstzunehmen. Denkverbote sind also nicht nur bei der Auseinandersetzung mit den Rechtmäßigkeitsvoraussetzungen und Spielarten der Ermittlungsmaßnahmen verboten, gleiches gilt für die konkrete Umsetzung des Grundrechtsschutzes. Dieser ist wertlos, wenn er praktisch nicht ernst genommen wird oder strafverfolgungspraktischen Erwägungen weichen muss.

Zu den neuen Denkanstöße gehörten auf der Konferenz etwa ein kontradiktorisches Verfahren bei der Anordnung besonders intensiver Maßnahmen, indem z. B. ein Laie oder Datenschutzrechtler involviert wird, die tatsächliche ermittlungsrichterliche Tätigkeit sowie die Umsetzung anderer verfahrensrechtlicher Sicherungsmechanismen unabhängig evaluieren zu lassen oder auch ein erhöh-

[137] So Professor Dr. *Kyrill-Alexander Schwarz* in einer Stellungnahme vor dem Innenausschuss, 95. Sitzung, v. 11.03.2013, vgl. das Wortprotokoll S. 16. Die schriftlichen Stellungnahmen zur Novelle des § 113 TKG sind nicht mehr abrufbar.
[138] Die Grenze ist dort zu suchen, wo aus einer ex-ante-Betrachtung heraus die Anordnung noch vertretbar erscheint, vgl. *Bär*, TK-Überwachung, § 100a, Rn. 18.

ter „unterstaatlicher“ Druckmechanismus, der im Wege eines Whistleblower-Schutzes geschieht.[139]

Die „Evolution“ der Ermittlungsmaßnahmen verspricht auch in Zukunft Zündstoff für neue, erkenntnisreiche Diskussionen zu liefern. Jeder Einzelne ist aufgefordert, sich hieran zu beteiligen.

[139] Beispiel: Ein Unrechtmäßiges Vorgehen der Ermittlungsbehörden wird durch Insider zur Anzeige gebracht oder den Medien mitgeteilt ohne dass der Whistleblower straf- oder arbeitsrechtliche Konsequenzen zu befürchten hätte.

Die Überwachungspraxis des BND - Das Verfahren vor dem BVerwG

Philipp Wunderlin

Nahm man im Jahr 2014 eine Zeitung in die Hand, so konnte man sich einer Sache gewiss sein: Egal ob Clinton, Türkei oder „Maulwurf-Affäre“ – man stieß auf einen Artikel, der in mehr oder weniger empörter Weise über einen weiteren Fauxpas des Bundesnachrichtendienst (BND) berichtete.

So selbstverständlich diese kritische Berichterstattung derzeit erscheint, so ungewohnt und neu ist dieses angekratzte Image des BND doch. Denn über Jahrzehnte war der BND in der Öffentlichkeit in erster Linie als eine überaus verstaubte deutsche Behörde und Relikt aus Zeiten des kalten Krieges wahrgenommen worden. Schon die Bezeichnung „Bundesnachrichtendienst“ suggerierte ja in gewisser Weise, dass es sich lediglich um eine harmlose Behörde handelt, die mit Nachrichten "dient".

Selbst im vergangenen Jahr, als auf der ganzen Welt über die Geheimdienste und deren Machenschaften diskutiert wurde, war der BND für die Medien weitestgehend uninteressant. Der Fokus der Berichterstattung lag eindeutig auf der Bedrohung durch die US-Geheimdienste. Schnell war man in Medien und Öffentlichkeit zu einer einfachen Einteilung der Welt in ein gutes und ein böses Lager übergegangen. Auf der einen Seite die gewissen- und rücksichtslos agierende NSA – auf der anderen Seite der gute, jedenfalls aber harmlose BND.

Was genau der BND eigentlich machte, das wusste und interessierte lange Zeit kaum jemanden. Aber das war auch nicht wichtig. Denn eine Bedrohung stellten ja nur die anderen dar.

Bezeichnenderweise war es dann auch der Untersuchungsausschuss zur NSA, der - im Mai dieses Jahres - erstmalig zu einer öffentlichen Auseinandersetzung mit der Überwachungspraxis und den Befugnissen des BND führte und erste Zweifel an der klassischen Einteilung in Gut und Böse aufkommen ließ.

Dabei waren vom BND schon zuvor Töne zu hören, die hätten aufhorchen lassen sollen. So trat der derzeitige BND-Chef Gerhard Schindler seinen Posten 2012 mit dem Slogan „No Risk – No Fun“ an. Sicherlich nur ein flapsiger Kommentar, meinte man damals. Denn der öffentlichen Wahrnehmung nach, war der BND zu diesem Zeitpunkt noch immer nicht viel mehr als die etwas träge Behörde mit Schlapphut.

Tatsächlich waren aber bereits weit vor Snowden und der NSA Informationen aufgetaucht, die ein ganz anderes Bild vom BND zeichneten. Ein Bild von einem Geheimdienst, der bei seiner Schnüffelei – genau wie die angloamerikanischen Dienste – weder Rücksicht auf Grundrechte noch sonstige Normen nimmt. Eine Behörde, die über massive Überwachungskapazitäten verfügt und weitgehend befreit von gesetzlichen Schranken und gerichtlicher Kontrolle agiert.

1 Der Klageanlass

Anfang 2012 wurde aufgrund des jährlichen G10-Berichts des Parlamentarischen Kontrollgremiums (PKGr) bekannt, dass der BND im Jahre 2010 Auslands-E-Mails mit ca. 30.000 Suchbegriffen durchsucht hatte. Dabei handelte es sich laut dem Bericht des PKGr bei den Suchbegriffen um „gängige und mit dem aktuellen Zeitgeschehen einhergehende Begriffe". Die Suche hatte zu rund 37 Mio. „Treffern" geführt, die „nachrichtendienstlich bearbeitet" wurden.[1]

Damit hatte sich die Zahl der Treffer – d.h. E-Mails die einen der Suchbegriffe enthielten – im Vergleich zum Vorjahr mehr als verfünffacht. Von diesen Treffern wurden gerade einmal 12 E-Mails als „nachrichtendienstlich relevant" eingestuft. Mit anderen Worten: Um 12 „relevanten" E-Mails auf die Spur zu kommen, waren etliche Milliarden E-Mails durchforstet worden!

Die Überwachungsmaßnahmen haben ihre formelle gesetzliche Legitimierung in § 5 Abs. 1 G10, der wie folgt lautet:

(1) Auf Antrag des Bundesnachrichtendienstes dürfen Beschränkungen für internationale Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt, angeordnet werden. Die jeweiligen Telekommunikationsbeziehungen werden von dem nach § 10 Abs. 1 zuständigen Bundesministerium mit Zustimmung des Parlamentarischen Kontrollgremiums bestimmt. (…)

Hinter dieser etwas kryptischen Vorschrift verbirgt sich die weitreichendste Überwachungsmaßnahme, die in Deutschland rechtlich möglich ist. Der BND darf im Prinzip alle „internationalen Telekommunikationsbeziehungen" überwachen.

[1] Bericht vom 10.2.2012, BT-Drs. 17/8639.

Eine besondere Qualität kommt der Überwachung dabei insbesondere aus drei Gründen zu:

- die Überwachung erfolgt anlass- und verdachtslos;
- die Maßnahmen erfolgen heimlich, ohne dass sie den Betroffenen – vorab oder im Nachhinein - zur Kenntnis gelangen;
- der BND braucht für Abhörmaßnahmen keinerlei gerichtliche Erlaubnis und § 13 G10 schließt den Rechtsweg weitgehend aus.

2 Das Verfahren vor dem Bundesverwaltungsgericht

Aufgrund des Berichts des PKGr hatte Rechtsanwalt *Niko Härting* bereits im Februar 2013 – und somit lange vor Aufflammen des NSA Überwachungsskandals – in eigenem Namen Klage beim Bundesverwaltungsgericht (BVerwG) gegen die Bundesrepublik Deutschland als Rechtsträger des BND eingereicht.

Angesichts der hohen Zahl der vom BND kontrollierten E-Mails musste er davon ausgehen, dass auch seine Kommunikation von den Maßnahmen des BND betroffen war. Denn er hatte 2010 in erheblichem Umfang per E-Mail mit ausländischen Mandanten und Kollegen kommuniziert – teilweise auch mit Personen aus vermeintlichen „Krisenregionen", bei denen Maßnahmen des BND mit besonders hoher Wahrscheinlichkeit zu erwarten waren.

Mit der Klage beantragte er, festzustellen, dass der BND im Jahre 2010 das Fernmeldegeheimnis des Klägers verletzt hatte, indem er im Zuge der strategischen Fernmeldeüberwachung seinen E-Mail-Verkehr erfasst und weiterbearbeitet hatte.

Angesichts der immensen Anzahl überwachter E-Mails und dem verschwindend geringen Output von lediglich 12 E-Mails mit nachrichtendienstlicher Relevanz drängte sich eine Verletzung des Grundsatzes der Verhältnismäßigkeit geradezu auf. Die Schwere des Grundrechtseingriffs war dabei insbesondere darauf zurückzuführen, dass die Überwachungsmaßnahmen anlass- und verdachtslos erfolgen und es zudem faktisch an jeglicher Benachrichtigungspflicht fehlt. Das daraus resultierende diffuse Gefühl des ständigen Überwachtwerdens und mögliche Chilling Effects auf das Kommunikationsverhalten schienen im Hinblick auf Art. 10 GG besorgniserregend.

Darüber hinaus wurde eine Verletzung des Anwaltsgeheimnisses gerügt, da es laut Angaben des BND keinerlei Vorkehrungen gibt, die eine Vertraulichkeit anwaltlicher Mails gewährleisten.

2.1 Die Verteidigung des BND

Der BND stützte seine Verteidigung im Wesentlichen auf zwei Argumente: Auf Zulässigkeitsebene wurde dem Kläger das Fehlen eines substantiierten Vortrags vorgeworfen. Paradoxerweise wies der BND gleichzeitig jegliche Forderung nach Aufklärung der Maßnahmen und Einsicht in die Protokolle zurück. Anstatt Antworten zu geben, beschränkte sich der BND darauf, den sämtlichen klägerischen Vortrag zu bestreiten. Auf Begründetheitsebene begnügte sich der BND sodann schlichtweg damit, in großzügiger Weise auf die Entscheidung „Telekommunikationsüberwachung" aus dem Jahr 1999 zu verweisen, in welcher das *BVerfG* die strategische Fernmeldeüberwachung im Kern für verfassungsgemäß erachtet hatte.[2]

Dabei ignorierte der BND jedoch einige ganz wesentliche Punkte:

Die Karlsruher Richter hatten das G 10-Gesetz 1999 in Teilen für verfassungswidrig erklärt und den Gesetzgeber in etlichen Punkten zu Nachbesserungen verpflichtet. Eine verfassungsrechtliche Überprüfung des G 10-Gesetzes in seiner derzeitigen Fassung hatte indes nie stattgefunden.

Darüber hinaus waren die technischen Möglichkeiten, die 1999 noch einen wesentlichen begrenzenden Faktor darstellten, zwischenzeitlich größtenteils weggefallen. Aus der Gesetzesbegründung des aktuellen G 10-Gesetzes geht hervor, dass es im Zeitpunkt der Erweiterung des G 10-Gesetzes im Jahr 2001 lediglich möglich war, 750 Auslandstelekommunikationen (alle Medien) pro Tag überhaupt zu kontrollieren. Im Jahr 2010 waren es hingegen bereits

[2] *BVerfGE* 100, 313.

100.000 Auslandskommunikationen pro Tag (nur E-Mails), die einen „Treffer“ enthielten.

Zudem wurde die strategische Fernmeldeüberwachung im Rahmen der G 10-Novelle 2001 erheblich ausgeweitet und geht in vielen Bereichen deutlich über den Regelungsbereich der Entscheidung des Bundesverfassungsgerichts aus dem Jahr 1999 hinaus. Während bis 2001 nur satellitengebundene Telekommunikation überwacht werden durfte, erweiterte die G 10-Novelle die Befugnisse des BND auch auf leitungsgebundene Telekommunikation. Zugleich wurde dem BND die Befugnis eingeräumt, bis zu 20 % der Telekommunikation zu überwachen. Dies, obwohl das *BVerfG* im Jahr 1999 die prinzipielle Verfassungsmäßigkeit des G 10 noch u.a. damit begründet hatte, dass aus technischen Gründen maximal 10 % des Auslands-Fernmeldeverkehrs überwacht werden konnte.

Außerdem wurde die Benachrichtigungspflicht erheblich gelockert, welche bei der aktuellen Gesetzeslage nun die absolute Ausnahme darstellt. Seit 2001 ist der BND im Normalfall nicht mehr verpflichtet, die Betroffenen von Maßnahmen der strategischen Fernmeldekontrolle in Kenntnis zu setzen. Nach § 12 Abs. 2 Satz 1 G10-Gesetz erfolgt eine Mitteilung nur noch in den Fällen, in denen Daten nicht unverzüglich gelöscht werden.

Besonders gravierend ist jedoch, dass bei genauerer Beleuchtung letztlich keiner der gesetzlich vorgesehenen Begrenzungsfaktoren eine effektive Begrenzung der Fernmeldeüberwachung gewährleistet.

2.2 Internationale Kommunikation

Das *BVerfG* hatte die Beschränkung auf internationale Telekommunikation 1999 noch als einen der maßgeblichen Faktoren hervorgehoben, der die Verhältnismäßigkeit der strategischen Fernmeldeüberwachung gewährleistet.

Insbesondere im Bereich der Internetkommunikation war es aber seit jeher zweifelhaft, ob sich eine derartige „Beschränkung“ überhaupt trennscharf handhaben lässt. Angesichts der Äußerungen des BND in der Verhandlung vor dem *BVerwG* verblasste dann aber auch der vage Glaube daran, dass die gesetzlich geforderte Selektion zwischen nationalen und internationalen Verkehren im Bereich der Internetkommunikation unter heutigen technischen Bedingungen überhaupt durchführbar ist. Der BND-Vertreter erklärte nämlich, eine maschinelle Sondierung stieße prinzipiell schon dann an ihre Grenzen, wenn es um E-Mails ginge, die von einer „.com“-Domain aus versandt und über einen ausländischen Server geleitet werden.

2.3 „Gebündelte Übertragung“

Die Vorgabe in § 5 Abs. 1Satz 1 G 10, Telekommunikationsbeziehungen dürften nur insoweit überwacht werden, als eine gebündelte Übertragung erfolgt, ist praktisch bedeutungslos. Denn „nicht-gebündelt“ wird Telekommunikation nur noch auf dem letzten Leitungsabschnitt der einzelnen Teilnehmeranschlussleitung bzw. auf der Mobilfunkstrecke zwischen dem einzelnen Endgerät und der Funkzelle übertragen. Auf diesen individualisierten Übertragungswegen kann aber eine strategische Beschränkung ohnehin nicht ansetzen, da sie sich gerade nicht gezielt gegen einzelne Personen richten darf.

2.4 „20%-Grenze“

Der BND musste selbst einräumen, dass Bezugspunkt der Obergrenze nicht etwa das tatsächliche Übertragungsvolumen ist, sondern die absolute Übertragungskapazität. Da die tatsächliche Auslastung einzelner Übertragungswege in aller Regel unter 20 % liegt, steht die „20%-Grenze“ einer Vollüberwachung daher nicht entgegen.

2.5 Suchbegriffe

Das G 10-Gesetz sieht keine Limitierung der Anzahl und Gängigkeit der verwendeten Suchbegriffe vor. Durch eine Erhöhung der Anzahl, vor allem aber durch die Wahl „gängiger mit dem Zeitgeschehen einhergehender Begriffe“ kann der BND die Überwachung praktisch beliebig ausweiten. Für die Verwendung von gängigen Alltagsbegriffen sprach auch, dass der explosionsartige Anstieg der Treffer im Jahr 2010 vom BND mit einer angeblichen „Spam-Welle“ begründet wurde, in deren Rahmen Spamnachrichten mit „zufälligen Auszügen aus Tagesnachrichten oder Internet-Blogs“ versehen waren.

Noch bedenklicher ist allerdings, dass im Bereich der Internetkommunikation das Verbot der Verwendung personenbezogener Suchbegriffe (§ 5 Abs. 2 Nr. 1 G 10) praktisch außer Kraft gesetzt ist. Bezugspunkt dieses Verbots sind Telekommunikationsanschlüsse. Ein Verbot der gezielten Erfassung bestimmter Telekommunikationsanschlüsse kann aber nur dann die gezielte Überwachung bestimmter Telekommunikationsteilnehmer verhindern, wenn Telekommunikationskontakte stets durch einen Bezug auf bestimmte Telekommunikationsanschlüsse (insbesondere durch eine Rufnummer) zugeordnet werden. Dies entspricht der Lage bei Telefonverbindungen, bei denen ein Telekommunikationsanschluss dauerhaft und eindeutig einer Rufnummer zugeordnet ist. E-Mail-Adressen und E-Mail-Postfächer hingegen beziehen sich nicht auf Telekommunikationsanschlüsse. Von welchem Telekommunikationsanschluss aus eine E-Mail versandt oder abgerufen wird, ist für die Individualisierung von Absender und Empfänger irrelevant. Ein E-Mail-Postfach kann vielmehr weltweit von jedem Telekommunikationsanschluss bedient werden. Der BND ist nach dem Wortlaut des § 5 G 10 dazu befugt, E-Mail-Adressen – die in der Regel einzelnen Personen zugeordnet sind – als Suchbegriffe zu verwenden. Von dieser Möglichkeit macht der BND laut eigenen Angaben umfassenden Gebrauch. Diese Praxis steht nicht in Widerspruch zu § 5 G 10, obwohl die grundrechtliche

Gefährdungslage nicht weniger schwer wiegt als etwa bei einer Auswertung mittels bestimmter Telefonnummern.

Bemerkenswerterweise hatte das *BVerfG* in der G 10-Entscheidung aus dem Jahr 1999 noch betont, dass dem Verbot der gezielten Überwachung bestimmter individueller Anschlüsse besondere Bedeutung zukommt: „Ohne ein solches Verbot wäre die Verhältnismäßigkeit angesichts der Verdachtslosigkeit der Eingriffe, der Breite der erfaßten Fernmeldekontakte und der Identifizierbarkeit der Beteiligten nicht gewahrt".[3]

Besonders schockierend war in diesem Zusammenhang die Veröffentlichung einer Liste von Ländern, die 2010 (und vermutlich bis heute) von der Auslandsüberwachung des BND betroffen sind. Zwar soll laut Gesetz auch die Begrenzung der Maßnahme auf den Verkehr mit bestimmten Gebieten eine minimierende Wirkung haben. Davon kann in der Praxis aber nicht die Rede sein. Immerhin erfasst die BND-Überwachung den Telefon- und Emailverkehr mit 196 Ländern. Neben klassischen „Schurkenstaaten" stehen auch die USA, Frankreich, England und nahezu alle anderen europäischen Länder auf der Liste. Der in der Verhandlung anwesende Stellvertretende Vorsitzende der G 10-Kommission, Bertold Huber, bekundete, dass sich die G 10-Kommission in diesem Punkt auf die Kontrolle durch das PKGr verlasse. Sowohl das PKGr als auch das Bundeskanzleramt hatten in der Vergangenheit die Erstreckung der Überwachung auf 196 Länder der Welt aber bedenkenlos „durchgewunken".

[3] *BVerfGE* 100, 313, 384.

3 Die Entscheidung des BVerwG

Zu einer Auseinandersetzung mit dem oben Vorgebrachten sollte es letztlich aber gar nicht kommen. Das BVerwG hielt die Klage bereits für unzulässig, weil „nicht mit an Sicherheit grenzender Wahrscheinlichkeit" festzustellen sei „dass Telekommunikationsverkehre des Klägers erfasst worden sind".[4]

Die Begründung für diese Einschätzung musste überraschen. Denn nach Ansicht des *BVerwG* sei es für die Wahrscheinlichkeit der Betroffenheit „unerheblich, dass die größten deutschen Telekommunikationsdienstleister abgewickelt werden, (…) und Telekommunikationsverkehre in und aus 196 Ländern beschränkt worden sind", denn die Überwachungsmaßnahmen seien „schon dann wirksam begrenzt, wenn nur 20 v.H. der Kapazität aller beantragten und angeordneten Übertragungswege überwacht werden dürfen".[5] Art. 19 Abs. 4 GG gebiete es nicht, das Beweismaß auf weniger als die „volle richterliche Überzeugung" abzusenken. Die Unerweislichkeit der Betroffenheit – und damit der faktische Ausschluss des Rechtsschutzes – sei deswegen zumutbar, weil die Kontrollpflichten und -befugnisse der G10-Kommission einen „kompensatorischen Grundrechtsschutz" böten.[6]

[4] *BVerwG* vom 28.05.2014, Az. 6 A 1.13, Rn. 25.
[5] *BVerwG* a.a.O., Rn. 29.
[6] *BVerwG* a.a.O., Rn. 40.

4 Analyse des Urteils

Das Urteil weist gravierende Schwachstellen auf.

Zunächst hat das BVerwG dem Kläger die Beweislast für die eigene Betroffenheit aufgebürdet, ohne sich zuvor in der gebotenen Weise um Aufklärung des Sachverhalts zu bemühen und ohne sich mit den Gesichtspunkten auseinanderzusetzen, die im Interesse der Effektivität des Rechtsschutzes (Art. 19 Abs. 4 GG) bei der Zuordnung von Beweislasten von Verfassungs wegen berücksichtigt werden müssen. Damit hat das BVerwG wesentliche Elemente des tatsächlichen Vortrages und der rechtlichen Argumentation des Klägers nicht zur Kenntnis genommen und in seiner Entscheidung nicht gewürdigt.

Dies, obwohl das *BVerfG* in ständiger Rechtsprechung statuiert, dass die fachgerichtliche Überprüfung grundrechtseingreifender Maßnahmen den effektiven Schutz der berührten materiellen Rechte nur gewährleisten kann, wenn sie auf zureichender Aufklärung des jeweiligen Sachverhalts beruht.[7]

Zudem verneinte das BVerwG die Klagebefugnis des Klägers auch entgegen jeglicher tatsächlichen Wahrscheinlichkeit. Denn selbst wenn man davon ausginge, dass der BND lediglich jede einhundertste (Auslands-) E-Mail überwacht, läge die Wahrscheinlichkeit, von der Überwachung erfasst zu werden, denkbar hoch: Bei einer Person, die, 100 Auslands-E-Mails verschickt hat, bei 63,4 %; bei 1.000 E-Mails bereits bei 99,9 %. Das Urteil des BVerwG beruhte daher auf Erwägungen, die nicht nachvollziehbar sind und gegen Art. 3 Abs. 1 GG in seiner Bedeutung als Willkürverbot verstoßen. Darüber hinaus hat das BVerwG durch die überstrenge Handhabung des § 43 VwGO den Rechtsschutz gegen Grundrechtseingriffe, die der BND im Zuge der strategischen Fernmelde-

[7] Vgl. *BVerfGE* 101, 275.

überwachung vornimmt, faktisch ausgeschlossen und dadurch jeglichen Rechtsschutz leerlaufen lassen. Insofern verkennt die Entscheidung des BVerwG wesentliche Grundsätze der Garantie effektiven Rechtsschutzes und übersieht die diesbezügliche Rechtsprechung des *BVerfG*. Denn laut *BVerfG* verlangt Art. 19 Abs. 4 GG, dass die Gerichte ein von der Rechtsordnung eröffnetes Rechtsmittel nicht durch eine überstrenge Handhabung verfahrensrechtlicher Vorschriften ineffektiv machen und für den Kläger "leer laufen" lassen dürfen.[8]

Das vom BVerwG geforderte Beweismaß hinsichtlich einer tatsächlichen Betroffenheit führt effektiv aber dazu, dass nur diejenigen ein Klagerecht haben, deren Nachrichten als „nachrichtendienstlich relevant“ eingestuft werden. Im Jahr 2010 wären dies lediglich 12 von insgesamt 37.000.000 Betroffenen gewesen. Wäre die vom BVerwG geäußerte Auffassung zutreffend, gäbe es faktisch keinen Rechtsschutz gegen Überwachungsmaßnahmen nach § 5 G10.

[8] *BVerfG*, Beschluss vom 2.12.1987, Az. 1 BvR 1291/85.

5 Fazit

Das vom BVerwG geforderte Beweismaß machte es nicht nur dem klagenden Rechtsanwalt Niko Härting, sondern praktisch jedem der Millionen, die von den Überwachungsmaßnahmen des BND betroffen sind, unmöglich, Rechtsschutz gegen den erlittenen Grundrechtseingriff zu erlangen. Trotzdem kommt eine Absenkung des Beweismaßes für das Gericht nicht in Betracht. Zu groß die Sorge um „justizielle Entscheidungsressourcen und eine (angebliche) „faktische[n] Ermöglichung einer Popularklage".[9] Festzustellen bleibt, dass das BVerwG sich einer Auseinandersetzung mit den spezifischen Umständen des Sachverhalts verschlossen und dabei einen wesentlichen Grundsatz der Garantie effektiven Rechtsschutzes verkannt hat. Denn Art. 19 Abs. 4 GG gewährleistet nicht nur das formelle Recht, die Gerichte anzurufen, sondern statuiert auch eine tatsächlich wirksame gerichtliche Kontrolle.

[9] *BVerwG* vom 28.05.2014, Az. 6 A 1.13, Rn. 41.

Packet Inspection in Zeiten von Big Data

Agata Królikowski

Deep Packet Inspection (DPI) bündelt verschiedene Internet-Technologien, die tiefgreifende Einschnitte in die informationelle Selbstbestimmung jedes Einzelnen ermöglichen. Wie ist es möglich, dass eine solche Technologie nahezu am öffentlichen Diskurs vorbei in die Netzinfrastruktur eingebettet werden konnte? Diese Frage ist der Ausgangspunkt des folgenden Beitrags.

Über das Internet versendete Informationen werden mittels DPI analysiert und verwaltet. Dabei können nicht nur Verkehrsdaten, sondern auch Inhalte wie beispielsweise persönliche Nachrichten der Nutzer ausgewertet werden. Die Anwendungsmöglichkeiten sind vielfältig. Sie reichen von der Abwehr von Angriffen auf Netzwerke über das Abhören von Kommunikation hin zum Blockieren von Informationen. Und je mehr Daten zur Verfügung stehen, desto besser werden die Verfahren. Längst hat dabei DPI Eingang in viele Bereiche unseres täglichen Lebens gefunden, ohne dass die meisten etwas davon ahnen.

Im folgenden Beitrag werden zunächst die wichtigsten technischen Grundlagen der DPI erläutert, um verständlicher zu machen, dass und inwiefern auf der digitalen Ebene ein Schutz privater Daten vor DPI kaum realisierbar ist. Schließlich werden die rechtliche Verankerung von DPI und die insgesamt damit einhergehenden gesellschaftlichen Herausforderungen diskutiert.

1 Paketbasierte Kommunikation

Moderne Netze wie das Internet sind paketbasierte Netze. Alle Nachrichten, die wir über das Internet verschicken, werden in Pakete unterteilt und mit Hilfe des *Routings*[1] zum Empfänger geschickt. Pakete wiederum sind logisch in sogenannte Schichten (nach dem *OSI-Referenzmodell*[2] (bzw. im Internet nach dem *TCP/IP-Modell*)[3] aufgeteilt, vgl. Abbildung 1.[4] Jede Schicht besteht aus einem Protokollkopf und dem Inhalt. Die unterste Schicht 1 bildet dabei die Bitübertragungsschicht, auf der die Informationen transportiert werden, die oberste Schicht 7 ist die Anwendungsschicht. In dieser Schicht befinden sich die eigentlichen vom Nutzer erzeugten Inhaltsdaten wie z. B. E-Mails, die mit den Protokollinformationen der jeweiligen Schicht von oben nach unten angereichert werden. Je „höher" die Schicht, desto „tiefer" liegt die entsprechende Information im Paket verborgen, vgl. Abbildung 3.

[1] Wegebestimmung von Paketübertragungen.
[2] Open Systems Interconnection.
[3] Transmission Control Protocol / Internet Protocol.
[4] Vgl. *Tanenbaum*, Computernetzwerke, 2003, S. 52.

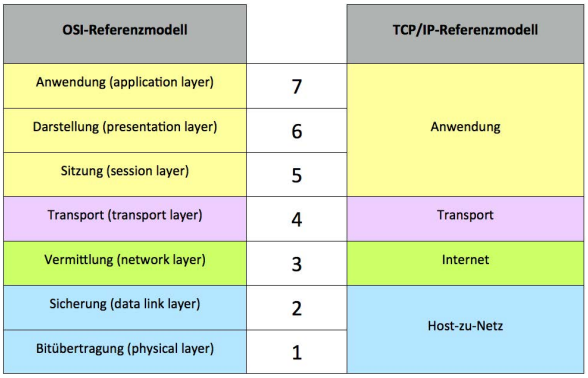


Abbildung 1

Die OSI- und TCP/IP-Referenzmodelle, vgl. *Tanenbaum*, Computernetzwerke, 2003, S. 60.

Damit Netze wie das Internet funktionieren, müssen Teile der Paketschichten – genauer: die Steuerdaten (z. B. die IP-Adresse für das Routing) – ausgewertet werden.

Die Auswertung der Steuerdaten (aber auch der Inhaltsdaten) kann auch dazu genutzt werden, Pakete in verschiedene Klassen einzuteilen und die Klassen entsprechend bestimmter Regeln zu behandeln. Diese Regeln können das Verzögern, Priorisieren oder Löschen einzelner Paketklassen beinhalten. Darin liegt im Wesentlichen die Idee sogenannter Paketfilter.

Erste Paketfilter sind Mitte der 1970er Jahre aufgekommen. Bereits Anfang der 1980er wurden dann auch Paketfilter in Form von *Firewalls* implementiert,[5] doch erst im Jahre 1988 – mit dem Aufkommen der als Morris-Wurm bekannt gewordenen Schadsoftware und damit des ersten flächendeckenden Angriffs auf Computer[6] – zeigte sich, dass Netze Paket- und damit Informationskontrollen brauchten. Mit jeder neuen Generation solcher Filter wurde der Schutz der Netze stetig weiterentwickelt und aufgrund steigender Rechen- und Speicher-

[5] Vgl. *Ingham/Forrest,* A History and Survey of Network Firewalls, 2002, S. 2.
[6] Vgl. *Ingham/Forrest* (Fn. 5) S. 4 m.W.N.

kapazität immer effizienter. Dabei wurde ein immer tieferer Blick in die Pakete möglich. Der Funktionsumfang des Open-Source-Netzwerkanalysewerkzeugs „Wireshark“[7] lässt erahnen, was Paketfilter der heutigen Generation können, vgl. Abbildung 2. Werkzeuge wie Wireshark sind in der Netzwerkadministration unerlässlich.

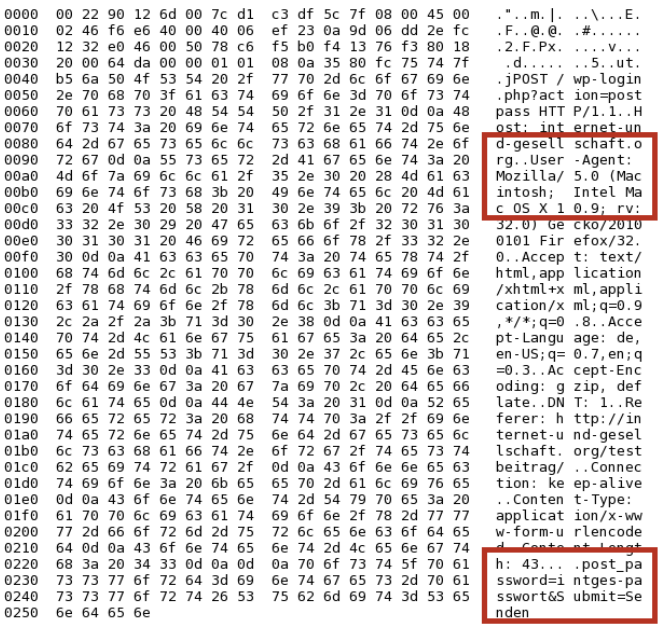


Abbildung 2

Zu sehen ist der Inhalt eines einzelnen IP-Paketes, aufgenommen mit der Software Wireshark. Bei diesem Inhalt handelt es sich um ein an eine Webseite über das Protokoll HTTP gesendetes Passwort. Die Kommunikation ist nicht verschlüsselt, das Passwort im Klartext sichtbar. Sichtbar sind auch andere Parameter wie Betriebssystem(version), Browser(version) und weitere Benutzereinstellungen.

[7] https://www.wireshark.org.

2 Paketfilter: Stand der Technik

Inzwischen ist die Entwicklung der Paketfilter bei den mit *Deep Packet Inspection* (DPI) bezeichneten Systemen angekommen. Der Begriff „tief“ bzw. „deep“ bezieht sich auf den Ort der Information in einem Paket mit Bezug auf die Schichten im OSI-Modell. Entsprechend gibt es auch die Begriffe *Shallow* und *Medium Packet Inspection*.[8]

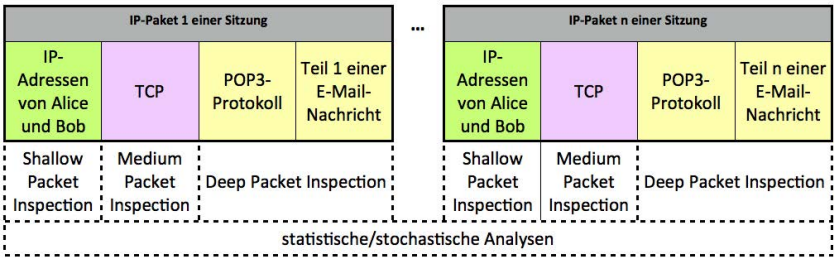


Abbildung 3

IP-Paketstrom und Ebenen der Paketanalyse

DPI ist ein Oberbegriff für verschiedene Paketfilter-Technologien, die es im Zusammenspiel miteinander ermöglichen, ganze Pakete und Paketströme zu filtern. Dies geschieht zum einen mit Hilfe der klassischen DPI, welche in der Lage ist, jedes einzelne Bit eines Pakets zu analysieren und das Paket in Abhängigkeit des Analyseergebnisses zu klassifizieren. Zum anderen werden mit Hilfe der *Statistical/Stochastic Packet Inspection* (SPI) statistische Parameter sowie Wahrscheinlichkeitsverteilungen berechnet und Pakete sowie Paketströme auf bestimmte Eigenschaften hin untersucht. Dabei können Paketlängen, zeitliche Abstände der Pakete oder generell Muster der Paketströme zur Klassifikation

[8] Vgl. *Porter*, The Perils of Deep Packet Inspection, 2010.

genutzt werden.[9] Diese Analysen können die gesamte Internetkommunikation einschließlich aller vom Nutzer erzeugten Daten wie z. B. Chatnachrichten, E-Mails, besuchte Webseiten, heruntergeladene Filme oder verwendete Passwörter über gewisse Zeiträume hinweg umfassen. Vereinzelt findet man dafür auch den Begriff der *Deep Content Inspection*.[10] Im Folgenden wird DPI als übergeordneter Begriff für Deep Packet Inspection, Statistical/Stochastic Packet Inspection und Deep Content Inspection verwendet.

DPI kann in jedem IP-basierten Netz eingesetzt werden und genügt heutzutage den Kriterien[11] von *Big Data* (*Volume*,[12] *Velocity* und *Variety*). Volume bezieht sich auf die Datenmenge, Velocity auf die Durchsatzrate und Variety auf die Heterogenität der Daten. Einen interessanten Überblick über die verschiedenen Anwendungen und Protokollarten, die ein solches System erkennen kann, liefert beispielsweise die Broschüre der Firma Ipoque.[13] Dort sind mehrere Hundert verschiedene Anwendungen und Protokolle genannt wie z. B. Skype, Spotify, SSH oder SSL. DPI-Systeme können Durchsatzraten von zu 600 Gbit/s erzielen.[14] Zum Vergleich: Einer der größten Internetknoten der Welt[15] – der Deutsche Commercial Internet Exchange Frankfurt (DE-CIX) – hat einen Durchsatz von etwa 1,76 Tbit/s.[16] Die Analysen sind damit theoretisch flächendeckend und darüber hinaus in Echtzeit, d. h. zum Zeitpunkt der Kommunikation, möglich, wenn man entsprechend viele solcher Maschinen an dem Knoten installieren würde.

---

[9] Vgl. *Hjelmvik/John*, Breaking and Improving Protocol Obfuscation, 2010, S. 24.
[10] Vgl. *Wedge Networks*, Deep Content Inspection With WedgeOS™, 2014.
[11] *Suciu* in: BNCOD, LNCS 7978, S. 1.
[12] So wurden 2012 schätzungsweise 2,5 Exybytes pro Tag erzeugt, vgl. *McAfee/Brynjolfsson* HBR, Oktober 2012, S. 62, 63. Eine gute Visualisierung von Datenmassen liefert beispielsweise *OpenDataCity*, Stasi versus NSA, 2013.
[13] Vgl. *Ipoque* Supported Protocols And Applications, 2013.
[14] Vgl. *Procera*, PacketLogic 20000 Platform, 2014.
[15] Vgl. *Packet Clearing House*, Internet Exchange Directory, 2014.
[16] Durchschnitt über den Zeitraum November 2013 – Oktober 2014, vgl. *DE-CIX Management GmbH*, Traffic Statistics, 2014.

3 Technischer Schutz aus Sicht des Endanwenders

Das Wireshark-Beispiel in Abbildung 2 zeigt, welche wichtige Rolle der Verschlüsselung in der Internetkommunikation zukommt, wenn es um das Schutzziel[17] der Vertraulichkeit geht. Dennoch stellt sich angesichts der technischen Möglichkeiten der DPI-Technologie die Frage, wie weit der technische Schutz eigentlich reicht. Dies hängt zum einen davon ab, was wir schützen wollen (Schutzziele),[18] zum anderen auch davon, vor wem.

DPI wird zuweilen als Technologie totalitärer Staaten dargestellt, deren Ausfuhr aus Deutschland höchstens reguliert werden müsste.[19] Wenig diskutiert wird hingegen, dass sie inzwischen ein wesentlicher Bestandteil der Infrastruktur ist. Zu den Anwendern gehören gleichermaßen Internet Service Provider (ISP), Anbieter von Mobiltelefonie, Ermittlungsbehörden, Geheimdienste, aber auch Institutionen wie beispielsweise Universitäten.[20] Beachtenswert ist auch die Vielseitigkeit des Einsatzes von DPI. Sie kann zum Schutz von Netzwerken gegen *Spam* und *Malware*, für *Quality of Service* bzw. *Traffic Management,* inhaltsabhängige Rechnungen, personalisierte Werbung, Sperren von Webinhalten und –diensten, aber auch zur gezielten Überwachung in Rahmen von Ermittlungsverfahren (lawful interception) genutzt werden. Die im Kern ver-

[17] *Eckert*, IT-Sicherheit. Konzepte, Verfahren, Protokolle, 2006, S. 6.
[18] Zum Begriff der Schutzziele vgl. z. B. *Pfitzmann/Rost* DuD 2009, 353 – 358.
[19] Vgl. z. B. *BT-Drs 17/8052*, 2011, S. 13 oder *Reporter ohne Grenzen*, Positionspapier von Reporter ohne Grenzen zum Export deutscher Überwachungstechnologie, 2012.
[20] Vgl. *Ipoque*, Case Studies, 2014.

wendeten Komponenten sind dieselben, lediglich die Ausbaustufen und Konfigurationen können sich unterscheiden.[21]

Unter diesem Aspekt betrachtet, ist es kaum verwunderlich, dass der Einsatz von DPI eine Reihe von Schutzzielen verletzt. So wird die Vertraulichkeit allein schon durch die Analyse der Pakete durch einen Mobilfunkanbieter oder ISP verletzt. Wenn Pakete aufgrund von Filterregeln verlangsamt oder gar verworfen werden, wird Nutzerkommunikation (unberechtigt) verändert und somit die Integrität verletzt. Schließlich ist auch das Schutzziel der Verfügbarkeit betroffen, wenn bestimmte Dienste – beispielsweise Videodownloads oder der Austausch über P2P[22]-Börsen – verlangsamt oder sogar gesperrt werden.[23]

An dieser Stelle soll beispielhaft der Schutz der Vertraulichkeit betrachtet werden. Diese kann man mit Hilfe von Verschlüsselungsmechanismen schützen, indem man Nachrichten so verändert, dass sie ohne weiteres nicht mehr lesbar sind. [24]

Dies kann in Form der Verbindungsverschlüsselung (engl. *link encryption)* oder der Ende-zu-Ende-Verschlüsselung (engl. *end-to-end encryption*) erfolgen. Bei der Verbindungsverschlüsselung wird das gesamte Paket zwischen Kommunikationspunkten verschlüsselt, so dass auch Sender und Empfänger verborgen bleiben. Allerdings müssen die beteiligten Router die Nachrichten entschlüsseln, um die Routinginformationen auszuwerten. Im Gegensatz dazu werden bei der Ende-zu-Ende-Verschlüsselung nur die Nutz-, nicht aber die Verbindungsdaten geschützt. Allerdings hat dies den Vorteil, dass die Nachrichten auch in den Routern verschlüsselt bleiben. Bei Verschlüsselungssystemen wie

[21] Vgl. z. B. *Procera* Internet Intelligence Products.
[22] Peer-to-Peer.
[23] Vgl. dazu z. B. die AGB von *Kabel Deutschland,* Internet und Telefon: Leistungsbeschreibung, Nr. 11 B.) und *Nederkoorn*, Verizon made an enemy tonight, 2014.
[24] Vgl. *Pfitzmann*, Sicherheit in Rechnernetzen, S. 151 oder *Eckert* (Fn. 17) , S. 744-749.

„GnuPG"[25] oder -protokollen wie „OTR"[26] (beide in der Anwendungsschicht angesiedelt) oder *SSL/TLS*[27] (für die Transportschicht) handelt es sich um Ende-zu-Ende-Verschlüsselung. Neben der Verschlüsselung des Klartextes ist es notwendig, Textmuster zu entfernen. Musteranalysen in Form statistischer Verfahren könnten sonst dazu führen, dass trotz der Verschlüsselung auf die ursprüngliche Nachricht geschlossen werden kann. Strukturen ergeben sich beispielsweise dadurch, dass bestimmte Buchstaben häufiger vorkommen als andere und sich das im Chiffrat widerspiegelt. Solche Redundanzen können mit Hilfe der Berechnung der Entropie ermittelt werden. Entropie ist ein Maß für die enthaltene Information in einer Nachricht. Je höher die Entropie ist, desto höher ist der Informationsgehalt. Maximale Entropie ist erreicht, wenn alle Bestandteile einer Nachricht (beispielsweise Buchstaben eines Alphabets) in gleichem Maße vorhanden sind, also eine Gleichverteilung vorliegt. Ein guter Verschlüsselungsmechanismus sollte in der Weise Strukturen unkenntlich machen, dass der verschlüsselte Text nicht von einer Zufallsfolge unterschieden werden kann. Gleichzeitig kann aber eine hohe Entropie wiederum als Filterkriterium für DPI-Maschinen dienen, verschlüsselte Kommunikation zu identifizieren.[28]

Als verschlüsselt erkannte Daten können dann entsprechend weiterbehandelt werden. Beispielsweise ist es denkbar, den Nutzer, der Verschlüsselungsmechanismen verwendet, besonders zu kennzeichnen und die Kommunikation für spätere Analysen zu speichern.[29] Ebenfalls ist es möglich, verschlüsselte Kommunikation grundsätzlich zu blockieren. Mitte Oktober 2014 gaben Techniker des VPN[30]-Anbieters Golden Frog Hinweise an die US-Regulierungsbehörde

[25] GNU Privacy Guard.
[26] Off-the-Record Messaging, URL: https://otr.cypherpunks.ca.
[27] Transport Layer Security / Secure Sockets Layer.
[28] Vgl. *Dorfinger et al.*, in*:* TMA'11, 2011, S. 168.
[29] Vgl. *Greenwald/Ball,* The Guardian, 20.6.2013.
[30] Virtual Private Network.

FCC[31] weiter, dass durch einen Mobilfunkanbieter verschlüsselte Pakete aktiv blockiert würden.[32]

Denn das Menschenbild, das häufig in der DPI-Forschung und auch seitens der -Hersteller und -Anwender der Technologie zugrunde liegt, ist auf den speziellen Anwendungsfall zugeschnitten, der sich aus der Geschichte der Paketfilter ableiten lässt, nämlich das des Nutzers als Angreifer:

„Such a system is particularly useful from a law enforcement application perspective since most of the time users with malicious intentions would try to hide their behavior either in encrypted or covert tunnels. Thus, systems that can classify encrypted traffic represent a first step in identifying such malicious users."[33]

Während Verschlüsselung nicht nur dazu dient, strafwürdige Inhalte im Internet zu verbergen, sondern einfach zum Schutz der Vertraulichkeit, hat sich das Bild des Nutzers kaum gewandelt.

Neben der gezielten Filterung, treten bei der Verschlüsselung noch weitere kritische Punkte auf. Ende-zu-Ende-Verschlüsselung ist zwar in der Lage, die konkreten Inhalte der Pakete (z. B. E-Mailnachrichten) unlesbar zu machen. Allerdings bleiben, wie oben beschrieben, die Umstände der Nachrichten bzw. die Verkehrsdaten (Sender, Empfänger, Uhrzeit, Standort etc.) in der Regel auswertbar. Dass aber solche Daten ausreichen, um detaillierte Profile einzelner Nutzer zu erstellen, findet im Telekommunikationsgesetz (TKG) bei der Erhebung solcher Daten Berücksichtigung und hat sich längst auch in der Rechtsprechung niedergeschlagen.[34]

---

[31] Federal Communications Commission.
[32] Vgl. *Thoma,* Golem.de vom 15.10.2014 sowie *Golden Frog,* Comments of The Golden Frog.
[33] *Alshammari/Zincir-Heywood*, in: Computer Networks 55 (6), 2011, S. 1326.
[34] *BVerfGE* 125, 260, 328.

Daneben ist zu bemerken, dass die konkreten Inhalte der Pakete für die Filterung nicht immer eine Rolle spielen müssen. Ein häufiger Anwendungsfall von DPI ist das Erkennen einzelner Anwendungsprotokolle trotz angewendeter Verschlüsselung mit Hilfe statistischer Analysen wie z. B. des P2P-Protokolls BitTorrent. Bei solchen statistischen Verfahren geht es nicht unbedingt darum, die darunter liegende Verschlüsselung zu brechen, sondern darum, gerade trotz verwendeter Verschlüsselungs- und Verschleierungsmechanismen die Informationen auswerten zu können (sog. Seitenkanalangriffe).[35] So werden beispielsweise im Vorfeld Daten über konkrete Implementationen von Verschlüsselungsalgorithmen gesammelt, die dabei helfen, die charakteristischen Eigenschaften von verschlüsselten Texten zu identifizieren und daraus Rückschlüsse auf den möglichen verschlüsselten Inhalt zu geben.[36] Dies erfolgt mit statistischen Methoden. Es liegt in der Natur der Kommunikation, dass jede verschlüsselte Nachricht eine Fülle von technischen Parametern besitzt (Länge der Pakete, Abstände, usw.), die analysiert und zur Filterung eingesetzt werden können. Es ist nicht möglich, alle Parameter von vornherein zu beeinflussen.[37]

Verschlüsselung erschwert die Auswertung der Inhalte von Kommunikation enorm und erhöht damit deren personellen, technischen und somit wirtschaftlichen Aufwand. Verhindern lassen sich die Analysen jedoch nicht. Ebenso wenig lässt sich verhindern, dass verschlüsselte Kommunikation unter besondere Filtermechanismen fällt. Zu hoffen bleibt jedoch, dass je mehr Nutzer Verschlüsselung einsetzen, sich zum einen der Analyse- und Speicheraufwand und damit Kosten noch weiter erhöhen und zum anderen die nichtverschlüsselte Kommunikation zum Ausnahmefall wird.

---

[35] Vgl. *Schmeh* Kryptografie*,* 2007, S. 262.
[36] Vgl. *Hjelmvik/John* (Fn. 9), S. 9, 10.
[37] Vgl. *Dyer et al.,* in: IEEE Symposium on Security and Privacy, 2012, S. 344. Nicht unerwähnt an dieser Stelle soll der Umstand bleiben, dass Fehler in den Implementationen von Software ausgenutzt werden, um die Verschlüsselung zu brechen. Dafür werden allerdings über DPI hinausgehende Verfahren eingesetzt, vgl. *Schneier,* Schneier on Security, 2013.

Die Herausforderung hierfür liegt jedoch darin, dass Nutzer sich in der Regel selbstverantwortlich auf ihren Endgeräten schützen müssen. Ein flächendeckender Schutz ist daher nur mit einer hohen Motivation der Nutzer erreichbar. Ein Hindernis hierbei ist, dass Datensicherheit und der daraus resultierende Schutz der Privatsphäre für viele Nutzer eine untergeordnete Rolle in der Nutzung ihres Computers spielen.[38] Ist die Verschlüsselungssoftware dann auch noch schwierig zu bedienen, kann von den meisten Nutzern nicht erwartet werden, dass sie sich mit den oben erwähnten Sicherheitsaspekten und Gefahren für Ihre Internetkommunikation beschäftigen.

Ein in dem DPI-Diskurs bisher kaum erwähntes Problem sind außerdem die Falschpositivraten der Filter. Zwar werden diese im Laufe des Einsatzes durch die Analyse von mehr Daten immer weiter verringert, können aber nicht gänzlich eliminiert werden. Falschpositive sind Pakete, bei denen ein bestimmter Inhalt eines Pakets erkannt wird, den das Paket nicht hat. Dies kann weitreichende Folgen haben. Ganz nach dem Thomas-Theorem „If men define situations as real, they are real in their consequences."[39] sind – obwohl Pakete falsch klassifiziert wurden, die Konsequenzen der Falschklassifizierung für den Nutzer real, wenn z. B. Pakete fälschlicherweise als P2P-Pakete erkannt und deswegen blockiert werden.[40] Dass Pakete falsch klassifiziert werden, kann nur dann festgestellt werden, wenn diese tatsächlich verworfen werden. Und auch dann sind die Verfahren aufwändig, denn Paketverluste sind in IP-Netzen an der Tagesordnung und können mit fehlender Bandbreite zusammenhängen, die zu einer zu geringen Durchsatzrate führen kann. Um einen Zusammenhang zu eingesetzten DPI-Maschinen herzustellen, bedarf es systematischer Analysen durch den Nutzer mit Hilfe spezieller Werkezuge. Ein Beispiel für ein solches

[38] *Whitten/Tygar,* in: Proceedings of the 8th Usenix Security Symposium, S. 172.
[39] *Thomas*, in: The Child in America: Behavior Problems and Programs. 1928, S. 572.
[40] In Werbebroschüren finden sich Formulierungen wie „unchallenged low false-positive rate", vgl. *Procera,* PacketLogic PL5600, 2014.

Werkzeug ist die Open-Source-Software „Glasnost“, welche auch von der „Initiative Netzqualität“ der Bundesnetzagentur zu Studienzwecken eingesetzt wurde.[41] Dennoch ist es für Nutzer kaum möglich, den Einsatz von DPI zu einem bestimmten Zeitpunkt nachzuweisen.

De facto sind Internetnutzer der DPI-Technologie weitestgehend ausgeliefert und ein technischer Schutz ist nur eingeschränkt möglich.

[41] Vgl. Netzneutralitätstest der BNetzA, URL: http://www.initiative-netzqualitaet.de/netzneutralitaetstest/ und Glasnost URL: http://www.measurementlab.net/tools/glasnost sowie *Dischinger et al.* in: Proceedings of the NSDI, 2010.

4 Rechtliche Implementation

Wenn es also nur einen bedingten technischen Schutz vor DPI gibt, stellt sich die Frage, ob es zumindest einen rechtlichen Schutz gegen DPI geben könnte. Der Ende 2013 geschlossene Koalitionsvertrag zwischen SPD und CDU gibt allerdings schon einen Hinweis darauf, dass dies im Moment nicht der Fall ist:

„Deep Packet Inspection (DPI) zur Diskriminierung von Diensten oder Überwachung der Nutzerinnen und Nutzer werden wir dagegen gesetzlich untersagen."[42]

Ein technischer Blick vornehmlich auf das TKG offenbart sogar, dass DPI nicht nur technisch, sondern auch rechtlich tief in der digitalen Netzinfrastruktur verankert ist.

So ist das Erheben von Verkehrsdaten gem. § 96 TKG zulässig, wenn dies für einen bestimmten Zweck des Abs. 1 Nr. 1-5 erforderlich ist. Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Bemerkenswert ist, dass Abs. 1 Nr. 3 explizit erlaubt, die Art des vom Nutzer in Anspruch genommenen Telekommunikationsdienstes zu erfassen, d. h. ob der Nutzer VoIP[43] nutzt oder eine Datei überträgt.[44] Diese Unterscheidung betrifft technisch gesehen die Anwendungsebene, d. h. sie ist ausschließlich mit Hilfe von DPI möglich. Ebenso nur mit DPI können die in § 96 Abs. 3 TKG erwähnten teilnehmerbezogenen Verkehrsdaten zum Zwecke der Vermarktung und zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten erhoben und entsprechend ausgewertet werden. Die geforderte Einwilligung können sich ISPs

[42] *CDU, CSU und SPD,* Koalitionsvertrag der 18. Legislaturperiode, S. 49.
[43] Voice over IP.
[44] Vgl. *Braun,* in: *Geppert/Schütz*, BeckTKG-Komm, 4. Aufl. 2013, § 96, Rn. 9.

bei Vertragsschluss geben lassen. So heißt es beispielsweise in den allgemeinen Geschäftsbedingungen von Kabel Deutschland:

„An den Knotenpunkten des Breitbandkabelnetzes werden automatisch Gesamt-Verkehrsvolumenmessungen durchgeführt. Grundsätzlich wird jede Art von Verkehr gleichmäßig durchgeleitet. Nur wenn die Gefahr einer Überlastung des Netzes besteht, ist Kabel Deutschland berechtigt, in den betroffenen Netzsegmenten den Verkehr zur Sicherung der Servicequalität folgendermaßen zu priorisieren: 1.) Zeitkritische Anwendungen (z. B. Video-Streaming, Internet-/Videotelefonie, Online-Gaming) erhalten Vorrang vor allen anderen Anwendungen, 2.) alle anderen Anwendungen (z. B. Internetsurfen, Social Network) haben immer Vorrang vor Filesharing-Anwendungen (z. B. Peer-to-Peer, One-Click-Hoster und Net-News).“[45]

Dass Qualitätsmaßnahmen möglich bleiben sollen, ist auch im Koalitionsvertrag vermerkt:

„Das sogenannte Best-Effort-Internet, das für die Gleichberechtigung der Datenpakete steht, wird in seiner Qualität weiterentwickelt und darf nicht von einer Vielzahl von „Managed Services“ verdrängt werden. Netzwerkmanagement muss allerdings dort möglich sein, wo es technisch geboten ist, damit bandbreitensensible Daten und Anwendungen verlässlich und ohne Verzögerung übertragen werden bzw. zum Einsatz kommen können.“[46]

Eine weitere rechtliche Implementation von DPI ist im Schutz vor Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten in § 100 TKG verborgen. Die Norm erlaubt in Abs. 1 das Erheben und Verwenden der Verkehrsdaten der Teilnehmer und Nutzer zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikati-

[45] Vgl. dazu bspw. die AGB von *Kabel Deutschland,* Internet und Telefon: Leistungsbeschreibung, Nr. 11 B.) 2. a.).
[46] Vgl. *CDU, CSU und SPD* (Fn. 41) ebd.

onsanlagen, soweit dies erforderlich ist. Laut Leitfaden des *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit* und der *Bundesnetzagentur* für eine datenschutzgerechte Speicherung von Verkehrsdaten können für diesen Fall alle Verkehrsdaten erhoben werden.[47]

Des Weiteren findet die rechtliche Implementation von DPI durch den Begriff „Stand der Technik" statt. Der Stand der Technik umfasst dabei die in der Praxis wissenschaftlich begründeten, praktisch erprobten und ausreichend bewährten Verfahren,[48] die hier eingangs dargestellt wurden. So wird der Stand der Technik in § 112 Abs. 3 im Zusammenhang mit dem automatisierten Auskunftsverfahren erwähnt, das durch eine Richtlinie der Bundesnetzagentur auszugestalten ist. Die Richtlinie der Bundesnetzagentur nimmt wiederum Bezug auf verschiedene Standardisierungsdokumente, und verweist damit auf entsprechende vorzuhaltende Technologie, die ihrer Beschreibung nach DPI-Funktionen innehat.[49] Im Allgemeinen kann man davon ausgehen, dass Überwachungsmaßnahmen mit Hilfe von DPI erfolgen.

Eine weitere Referenz auf diesen Begriff soll laut des Referentenentwurfs des Bundesministeriums des Innern zum sog. IT-Sicherheitsgesetz im § 109 Absatz 2 erfolgen. Die dort bisher beschriebenen technischen Maßnahmen zum Schutz gegen Störungen und Beeinträchtigungen müssen in Zukunft dem Stand der Technik entsprechen.[50] Auch hier ist der Stand der Technik die DPI-Technologie.

---

[47] Vgl. *BfDI/BNetzA*, Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten, S. 3.
[48] Vgl. *Eckhardt* in: Geppert/Schütz, BeckTKG-Komm, 4. Aufl. 2013, § 109, Rn. 31.
[49] Vgl. *ETSI* TS 101 331 V1.3.1, 2009, S. 10 und *ETSI* TS 102 232-1 V3.3.1, 2013, S. 41, dort wird die typische Funktionalität von DPI beschrieben.
[50] *BMI,* Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 18.8.2014, S. 19.

Die Verpflichtung der ISPs, eine Überwachungsinfrastruktur für den Staat, Schutzmaßnahmen gegen Störungen sowie die Erlaubnis, Qualitätssicherungsmaßnahmen bereitzuhalten, führt dazu, dass es grundsätzlich unmöglich wird, den Einsatz von DPI rechtlich einzudämmen.

Somit ist der Vorsatz aus dem Koalitionsvertrag, DPI zu verbieten zwar angesichts der technischen Möglichkeiten, die DPI bietet, um in die Privatsphäre der Nutzer einzudringen, lobenswert. Jedoch ist er angesichts der rechtlichen Verankerung der Technologie kaum realisierbar.

5 Fazit

Paketanalysen sind inzwischen sowohl für Klartexte als auch für verschlüsselte Daten in Echtzeit möglich. Die dafür notwendigen Geräte werden zur staatlichen Überwachung, Verwaltung von Netzressourcen sowie zu Abrechnungszwecken oder zum Schutz vor Spam-Mails und Malware als Firewall eingesetzt. Zwar kann man sich mit Verschlüsselung gegen Klartextanalysen schützen, gegen statistische Analysen sind jedoch auch Verschlüsselungsmechanismen weitgehend machtlos. Metadaten und Muster der Internetkommunikation lassen genügend Informationen, um daraus letztendlich auch Inhalte der Nachrichten abzuleiten. Es erfordert ein hohes Maß an technischem Verständnis, dies in der Alltagskommunikation zu berücksichtigen. De facto sind die meisten Nutzer dieser Technologie gegenüber machtlos.

Vor allem die Größenordnung, in der Daten in Echtzeit verarbeitet werden können, eröffnet dem, der die Daten kontrolliert, neue Spielräume. Der Unterschied zwischen Beobachten und Eingreifen, zwischen Information blockieren, Information verzögern oder Information durchleiten ist lediglich eine technische Regeldefinition in Software, die jederzeit geändert werden kann.

Diese Intransparenz stellt – zusammen mit der Größenordnung möglicher Analysen – eine neue Art der Kontrolle dar. Das Verhalten jedes einzelnen Nutzers kann detailliert aufgenommen, analysiert und gespeichert sowie mit anderen Daten verknüpft und rückwirkend auch in anderen Zusammenhängen betrachtet werden.

„In the ISP space, traffic classification techniques offer the possibility of identifying traffic patterns (which endpoints are exchanging packets and when), and

identifying what classes of applications are being used by a 'person of interest' at any given point in time."[51]

Da das Internet aber nicht nur ein Medium zur Kommunikation ist, werden dadurch viel mehr Facetten eines Nutzers erfasst als nur die Tatsache, wer mit wem wann worüber kommuniziert. Es wäre theoretisch möglich, ein „Meinungsbild der Nation" aufzunehmen und dieses auch zu steuern.

Es zeigt sich, dass mit dem Internet nicht nur Grenzen der Kommunikation verschoben, sondern mit der Digitalisierung auch die Hemmschwelle zur Überwachung deutlich gesenkt wurde.

Wenn es gegen DPI aber kaum einen technischen und juristischen Schutz gibt, bleibt am Ende die Frage, wie es um unsere Grundrechte im Internet überhaupt bestellt ist. Denn die technischen Möglichkeiten sind da und diese wecken Begehrlichkeiten, wie die Diskussion um das deutsche Mautsystem jüngst wieder zeigt.[52]

Möglicherweise sollten wir unsere bisherigen rechtlichen Vorstellungen über das Internet mit seinen Eigenschaften als Kommunikationsmedium, Radio, Fernsehen, Zeitung, Ausstellungs- oder Arbeitsort überdenken.

Aber auch aus technischer Sicht gilt es, Verfahren zu finden, die Prozesse wie Paketanalysen und -diskriminierung in einer Form sichtbar machen, die es auch Nicht-Experten erlaubt zu verstehen, was im Netz passiert. Denn *„[e]ine Freiheit, welche nur noch Experten offen steht, ist keine allgemeine Freiheit und kann keine Grundlage einer freien Informations- und Kommunikationsgesellschaft sein."*[53]

---

[51] *Nguyen/Armitage* Communications Surveys & Tutorials, IEEE 10 (4), S. 57.
[52] *Schröder,* Golem.de vom 27.10.2014.
[53] *Gusy* DuD, 2009, 35.

Dazu gehört, dass wir als Techniker lernen müssen, die Technik besser zu kommunizieren – sei es in Form besserer grafischer Benutzerschnittstellen, sei es durch nutzergerechte Sprache. Wir sollten bei der Entwicklung der Systeme im Hinterkopf behalten, dass wir etwas bauen, das für Menschen, an Menschen, in Menschen und gegen Menschen eingesetzt werden kann.

Edward Snowden hat uns gezeigt, dass diese Überlegungen nicht mehr in den einzelnen (Wissenschafts-)Communities erwogen werden dürfen. Der interdisziplinäre Austausch ist für die Entwicklung eines Auswegs aus der jetzigen Lage dringend erforderlich.

Literaturverzeichnis

Alshammari, R. & Nur Zincir-Heywood, A. (2010). Can encrypted traffic be identified wit- hout port numbers, IP addresses and payload inspection?, in: *Computer Networks,* Volume 55, Issue 6, 25, 1326–1350.

Bundesministerium des Innern (2014). *Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)* vom 18.8.2014.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bundesnetzagentur (2012). *Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten*. URL: http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenZumSpeichernVonVerkehrsdaten.pdf?__blob=publicationFile.

BT-Drs 17/8052. *Drucksache des Deutschen Bundestages vom 2.11.2011: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Katja Keul, Tom Koenigs, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 17/7738 –.* URL: http://dipbt.bundestag.de/dip21/btd/17/080/1708052.pdf.

CDU, CSU und SPD (2013). *Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD*, *18. Legislaturperiode*. URL: http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile&v=2.

DE-CIX Management GmbH (2014). *DE-CIX Traffic Statistics*. URL: https://www.de-cix.net/about/statistics/.

Dischinger, M. Marcon, M., Guha, S., Gummadi, K. P., Mahajan, R. & Saroiu, S. (2010). Glasnost: Enabling End Users to Detect Traffic Differentiation. In: *Proceedings of the USENIX Symposium on Networked Systems Design and Implementation (NSDI)*.

Dorfinger, P., Panholzer, G. & John, W. (2011). Entropy estimation for real-time encrypted traffic identification. In: *Proceedings of the Third international conference on Traffic monitoring and analysis* (TMA'11), Domingo-Pascual, J., Shavitt, Y. & Uhlig, S. (Hrsg.). Berlin, Heidelberg, Springer-Verlag, 164-171.

Dyer, K., Coull, S., Ristenpart, T. & Shrimpton, T. (2012). Peek-a-boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail. *Proceedings of the 33rd Annual IEEE Symposium on Security and Privacy*, 332–346.

Eckert, C. (2006). *IT-Sicherheit. Konzepte, Verfahren, Protokolle,* 4. Auflage, München, Oldenbourg Verlag.

ETSI (2009). *Lawful Interception (LI); Requirements of Law Enforcement Agencies.* TS 101 331 V1.3.1 (2009-10). URL: http://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.03.01_60/ts_101331v010301p.pdf.

ETSI (2013). *Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services.* ETSI TS 102 232-2 V3.4.1 (2013-02). URL: http://www.etsi.org/deliver/etsi_ts/102200_102299/10223202/03.04.01_60/ts_10223202v030401p.pdf.

Geppert, M. & Schütz, R. (Hrsg.) (2013). Beck'scherTKG-Kommentar, 4. Auflage, Müchen, C. H. Beck.

Gusy, C. (2009). Gewährleistung der Vertraulichkeit und Integrität informations- technischer Systeme – Neuer Grundrechtsname oder neues Grundrechtsschutzgut? *DuD 2009*, 33–41.

The Golden Frog (2014). *Comments of The Golden Frog*. URL: https://s3.amazonaws.com/s3.documentcloud.org/documents/1312218/golden-frog-comments-fcc-gn-14-28-final.pdf.

Greenwald, G. & Ball, J. (2013). The top secret rules that allow NSA to use US data without a warrant. *The Guardian* vom 20.6.2013, URL: http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant.

Hjelmvik, E. & John, W. (2010). *Breaking and Improving Protocol Obfuscation*, Technical Report No: 2010-05, Department of Computer Science and Engineering, Chalmers University of Technology, Gothenburg, Sweden.

Ingham, K., Forrest, S. (2002). *A history and survey of network firewalls*. URL: http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf.

Ipoque (2013). *Supported Protocols and Applications*, URL: http://www.ipoque.com/sites/default/files/mediafiles/documents/datasheet-supported-protocols.pdf.

Ipoque (2014). *Case Studies – Success stories*. URL: http://www.ipoque.com/en/resources/case-studies.

Kabel Deutschland (2014). *Allgemeine Geschäftsbedingungen, Internet und Telefon: Leitungsbeschreibung*. URL: http://www.kabeldeutschland.de/static/media/AGB_Internet_Telefon.pdf.

McAfee, A. & Brynjolfsson, E. (2012). Big Data: the Management revolution. In: *Harvard Business Review*, Oktober 2012, 60–68.

Nederkoorn, C. (2014). *Verizon made an enemy tonight*, URL: http://iamnotaprogrammer.com/Verizon-Fios-Netflix-Vyprvpn.html.

Nguyen, T. & Armitage, G. (2008). A survey of techniques for internet traffic classification using machine learning. *Communications Surveys & Tutorials*, IEEE 10 (4), 56-76.

OpenDataCity (2013). *Stasi versus NSA*, URL: http://apps.opendatacity.de/stasi-vs-nsa/.

Packet Clearing House (2014). *Internet Exchange Directory*. URL: https://prefix.pch.net/applications/ixpdir/.

Pfitzmann, A. (2000): *Sicherheit in Rechnernetzen, Mehrseitige Sicherheit in verteilten und durch verteilte Systeme*, 2000, URL: http://dud.inf.tu-dresden.de/~pfitza/DSuKrypt.pdf.

Pfitzmann, A. & Rost, M. (2009). Datenschutz-Schutzziele – revisited. DuD 2009, 353 – 358.

Porter, T. (2010). *The Perils of Deep Packet Inspection*, URL: http://www.symantec.com/connect/articles/perils-deep-packet-inspection.

Procera (2014). *Internet Intelligence Products*. URL: http://www.proceranetworks.com/products.

Procera (2014). *PacketLogic 20000 Platform*. URL: http://files.proceranetworks.com/resources/PL20000_082614_A4.pdf.

Procera (2014). *PacketLogic PL5600*. URL: http://www.daimler.fi/tuotteet/tietoliikenteen-hallintaratkaisut/procera/downloads/procera-datasheet-downloads/procera-packetlogic-5600.pdf.

Reporter ohne Grenzen (2012). *Positionspapier von Reporter ohne Grenzen zum Export deutscher Überwachungstechnologie*, URL: https://www.reporter-ohne-grenzen.de/fileadmin/rte/docs/Positionspapier.pdf.

Schmeh, Klaus (2007). *Kryptografie. Verfahren, Protokolle, Infrastrukturen.* 3. Auflage, Heidelberg, dpunkt.verlag.

Schneier, B. (2013). How to Remain Secure Against the NSA. *Schneier on Security*. URL: https://www.schneier.com/blog/archives/2013/09/how_to_remain_s.html.

Schröder, T. (2014). Polizei fordert Zugriff auf Mautdaten. *Golem.de* vom 27.10.2014, URL: http://www.golem.de/news/verbrechensbekaempfung-polizei-fordert-zugriff-auf-mautdaten-1410-110101.html.

Suciu, D. (2013). Big data begets big database theory. In: *Proceedings of the 29th British National conference on Big Data* (BNCOD'13). Gottlob, G., Grasso, G., Olteanu, D. & Schallhart, Ch. (Hrsg.). Springer-Verlag, Berlin, Heidelberg, 1–5.

Tanenbaum, A. S. (2003). *Computernetzwerke*. 4. Auflage. München, Pearson Studium.

Thoma, J. (2014). US-Provider blockiert verschlüsselte E-Mails*, Golem.de vom 15.10.2014,* URL: http://www.golem.de/news/netzneutralitaet-us-provider-blockiert-verschluesselte-e-mails-1410-109864.html.

Thomas W. I. (1928). The Methodology of Behavior Study. In: *The Child in America: Behavior Problems and Programs.* New York: Alfred A. Knopf (1928), 553–576, URL: http://www.brocku.ca/MeadProject/Thomas/Thomas_1928_13.html.

Wedge Networks (2014). *Deep Content Inspection With WedgeOS™*. URL: http://www.wedgenetworks.com/resources/technology/deep-content-inspection-with-wedgeos.html.

Whitten, A. & Tygar, J.D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. *Proceedings of the 8th Usenix Security Symposium*, 169–184.

Digitale Selbstverteidigung: Eine rechtliche Gratwanderung?

Sebastian Brüggemann

Wo der Staat seinen Schutzauftrag vernachlässigt, muss der Betroffene sein Recht auf Privatsphäre selbst verteidigen. Hier versprechen der Einsatz von Verschlüsselungssoftware und Anonymisierungsdiensten Abhilfe.

Viele dieser Dienste und Projekte sind aber auf die aktive Unterstützung ihrer Nutzer angewiesen. Doch wer aktiv ein Zeichen gegen staatliche Überwachung setzen will, dem drohen mitunter rechtliche Konsequenzen. Welcher Raum bleibt uns zwischen Störerhaftung und Hackerparagraph zur digitalen Selbstverteidigung? Sind das Hacken von Computersystemen oder DDoS-Attacken legitime Formen zivilen Ungehorsams oder nicht zu rechtfertigende Straftaten? Haben wir ein Recht auf Widerstand und wenn ja, in welchen Grenzen?

1 Einleitung

"Aus! Aus! Aus! [...] Big Brother – Das Experiment ist aus!"[1] Diese oder eine ähnliche Schlagzeile würden viele sicherlich nur allzu gerne im Zusammenhang mit der NSA-Affäre lesen. Die konnte jedoch kaum gemeint sein, tut die Politik doch bereits seit Monaten ihr Möglichstes, dieses unliebsame Thema zu begraben. Der *„Big Brother"* aus der Schlagzeile steht daher auch nicht für die vor kurzem wahr gewordene orwellsche Fiktion eines (totalitären) Überwachungsregimes, sondern für das bewegtbebilderte Affen-Selfie von TV-Unterhaltung. Sind wir vielleicht selbst schuld, weil wir uns am (digitalen) Selbstexibitionismus anderer erfreuen oder diesem in sozialen Medien fröhnen? Ist der Verzicht auf das Internet unsere letzte, vielleicht einzige Chance, der staatlichen Massenüberwachung zu entgehen? Wem es bei diesem Gedanken eiskalt den Rücken herunterläuft, hat nun eine deutliche Vorstellung davon, was sich hinter dem Begriff *„chilling effect"* [2] verbirgt. Vielleicht haben Sie tatsächlich nichts zu verbergen.

Nichts sehen, nichts hören, beredtes Schweigen. Während die Bundesregierung die Arbeit des mit der Aufklärung des Geheimdienstskandals betrauten Untersuchungsausschusses nach Kräften behindert, ist der Bürger auf sich allein gestellt. Wo der Staat sich aus der Verantwortung stielt, muss der Betroffene sein Recht auf Privatsphäre selbst verteidigen. Hierzu werden im Folgenden einige technische Möglichkeiten vorgestellt und auf ihre Tauglichkeit hin untersucht. Einige dieser Dienste und Projekte sind dabei auf die aktive Unterstützung ihrer Nutzer angewiesen, weshalb sich unweigerlich die Frage stellt, ob und wenn ja, welche rechtlichen Konsequenzen diese Art von Partizipation

[1] *Frank,* Spiegel Online v. 30.8.2014, http://www.spiegel.de/kultur/tv/promi-big-brother-finale-mit-roland-schill-bei-sat-1-a-988900.html.
[2] Ausführliche Informationen zum Thema *„chilling effects"* finden sich im gleichnamigen Beitrag von *Simon Assion* ab S. 31.

nach sich ziehen kann. Welcher Raum bleibt zur digitalen Selbstverteidigung? Auf diese Fragen versucht der folgende Beitrag eine Antwort zu finden.

2 Was soll die ganze Aufregung

Im Juni vergangenen Jahres berichteten der britische *Guardian* und die amerikanische *Washington Post* erstmals über die Überwachungsprogramme der National Security Agency (NSA) und des britischen Government Communications Headquarters (GCHQ). Auch über ein Jahr danach beherrscht das Thema noch immer die netzpolitische Diskussion. Geändert hat sich freilich wenig.

Auch wenn vieles nach wie vor im Unklaren liegt, gilt die flächendeckende, anlasslose Massenüberwachung der Internet- und sonstigen Fernmeldekommunikation durch die Geheimdienste als erwiesen. Zwischenzeitlich hat selbst der Generalbundesanwalt ein Ermittlungsverfahren eingeleitet, wenngleich auch nur, weil das Handy der Bundeskanzlerin abgehört wurde.[3] Die anlasslose Massenüberwachung deutscher Staatsbürger erscheint dagegen zu abstrakt. An der Frage des Nachweises der Betroffenheit scheiterte nicht zuletzt auch die Klage des Berliner Rechtsanwalts *Niko Härting* vor dem *BVerwG* in Leipzig.[4] Dieser fehlende Eindruck der subjektiven Betroffenheit ist es auch, der viele zu der Aussage verleitet, man habe doch nichts zu verbergen. Gleichwohl will eine Mehrheit der Deutschen ihren Chef nicht in sozialen Netzwerken befreunden[5] und spätestens beim Ausfüllen der Steuererklärung dürfte es vielen schwer fallen, sich dieses Credo wieder ins Gedächtnis zu rufen.

---

[3] *Pany*, Telepolis v. 4.6.2014, NSA-Überwachung: Der Generalbundesanwalt ermittelt, http://www.heise.de/tp/artikel/41/41932/1.html.
[4] Vgl. *BVerwG*, Urt. v. 28.5.2014, Az. 6 A 1.13, PM Nr. 35/2014.
[5] Zu diesem Ergebnis kommt eine im Auftrag des Bitkom e.V. durchgeführte Umfrage des Meinungsforschungsinstituts FORSA aus dem Jahr 2012, vgl. http://www.bitkom.org/de/presse/74532_70883.aspx.

2.1 Die Rolle der Geheimdienste

Die Rolle der Geheimdienste in einem demokratischen Staat ist geprägt von dem ambivalenten Verhältnis zwischen dem Sicherheits- und Freiheitsbedürfnis seiner Bürger. War im NSU-Verfahren der unzureichende Informationsaustausch zwischen den Verfassungsschutzbehörden Stein des Anstoßes, steht nun die vorbildliche Kooperation zwischen NSA und BND am Pranger.[6] Was auf den ersten Blick als widersprüchlich erscheinen muss, entpuppt sich bei näherer Betrachtung letztendlich nur als konsequent. Der erste Fall zeigt das Versagen der Dienste bei einer anlass- und einzelfallbezogenen Überwachungs- und Ermittlungsmaßnahme, wohingegen die anlasslose, massenhafte Überwachung beinahe der gesamten Internetkommunikation seit Jahren reibungslos funktioniert. Wo die gesamte Bevölkerung quasi unter Generalverdacht steht, dürfte es schwierig sein, einzelne Verdächtige auszumachen.

Bereits die Historie zeigt, dass das Verhältnis der Geheimdienste zur Demokratie ein eher angespanntes ist. Sie leisten einen wesentlichen Beitrag zur Aufklärung und Gefahrenprävention. Ihre Legitimationsgrundlage finden die deutschen Geheim- bzw. Nachrichtenddienste in Art. 87 Abs. 1 S. 2 GG. Dahinter steht das Bild einer *„streitbare(n), wehrhafte(n) Demokratie"*.[7] Probleme treten jedoch dort auf, wo sich die Tätigkeit der Geheimdienste der Kontrolle durch die ordentlichen Gerichte und damit dem Grundsatz der Gewaltenteilung entzieht. Wird zudem der Betroffene nach Abschluss der Überwachungsmaßnahme nicht informiert – was im vorliegenden Fall zugegebenermaßen einer Herkulesaufgabe gleichkäme – steht er faktisch rechtslos da. Während wir uns gegenüber dem eigenen Staat auf unsere Grundrechte und Verfassungsprinzipien berufen können, sind wir im Verhältnis zu ausländischen Geheimdiensten auf internationale Abkommen und Konventionen angewiesen. Fraglich ist, ob

[6] Ähnlich *Wunderlin* PinG 2013, 52.
[7] Vgl. *BVerfGE* 28, 36, 48 f.; *BVerfGE* 39, 334, 369 f.; *BVerfGE* 63, 266, 308 ff.; *Werthebach/Droste-Lehnen* DÖV 1992, 514 ff.

der Staat nicht verpflichtet ist, seine Bürger vor Grundrechtseingriffen ausländischer Geheimdienste zu schützen?

2.2 Die Schutzpflicht des Staates

Die anlasslose Massenüberwachung der Internetkommunikation deutscher Staatsbürger greift sowohl in das Fernmeldegeheimnis (Art. 10 GG, § 88 TKG) als auch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein. Beide gelten territorial unbeschränkt, weshalb es für die Annahme einer Verletzung lediglich eines Bezugs zu inländischen staatlichen Handelns bedarf,[8] wie bspw. des Informationsaustauschs zwischen NSA und BND. Beide sind als Abwehrrechte des Bürgers gegenüber Eingriffen der eigenen Staatsgewalt ausgestaltet.[9] Ausländische Geheimdienste sind folglich gerade nicht erfasst.[10]

In ihrer Eigenschaft als Freiheitsrechte sollen das Fernmeldegeheimnis und die informationelle Selbstbestimmung darüber hinaus eine möglichst freie Ausübung der Grundrechte gewährleisten. In Einzelfällen mag hieraus dem Staat eine objektive Pflicht erwachsen, seine Bürger vor Beeinträchtigungen Dritter zu schützen.[11] Dabei richten sich sowohl das Fernmeldegeheimnis als auch das Recht auf informationelle Selbstbestimmung gezielt gegen staatliche Überwachung. Darüber hinaus legen sie dem Staat eine Schutzpflicht im Verhältnis zu privaten Dritten auf,[12] die ihren Niederschlag im Bundesdatenschutzgesetz (BDSG) und dem Telekommunikationsgesetz (TKG) gefunden hat. Die Verletzung des einfachgesetzlichen Telekommunikationsgeheimnisses (§ 88 TKG) ist zudem strafbewehrt (§ 206 StGB). Wo das Abwehrrecht sich lediglich gegen

[8] *BVerfG* NJW 2000, 55 ff.
[9] *Klein*, NJW 1989, 1633, 1633; *Kipker/Voskamp* RDV 2014, 84.
[10] *Kipker/Voskamp* RDV 2014, 84.
[11] Ausführlich *Klein* NJW 1989, 1633, 1633 ff.
[12] *BVerfGE* 106, 28, 37; *Ewer/Thienel* NJW 2014, 30, 34.

Maßnahmen der eigenen Staatsgewalt richtet, gilt der aus den Grundrechten abgeleitete Schutzanspruch universell.[13] Maßgeblich ist ausschließlich die Frage, ob ein Eingriff in den grundrechtlich geschützten Bereich vorliegt, nicht von wem sie ausgeht.[14]

Sowohl das Fernmeldegeheimnis als auch das Recht auf informationelle Selbstbestimmung schützen die Dispositionsfreiheit des Individuums, frei von Zwang über die Preisgabe persönlicher Informationen zu entscheiden. Dies gilt sowohl für das „ob" als auch das „wie". Um hiervon Gebrauch zu machen, bedarf es jedoch der Kenntnis, welche Stelle welche Informationen jeweils erhebt, speichert und verarbeitet.[15] Wie die sukzessiven Enthüllungen im Zuge der NSA-Affäre jedoch gezeigt haben, fehlt es insbesondere im Bereich der Geheimdiensttätigkeit an der notwendigen Transparenz. Im Falle ausländischer Geheimdienste fehlt es neben einer rechtlichen Legitimationsgrundlage auch an der Möglichkeit einer nachträglichen, rechtlichen Überprüfbarkeit.[16] Es spricht daher vieles dafür, im vorliegenden Falle von einer Verpflichtung des Staates zum Schutz seiner Bürger auszugehen.[17] Freilich kommt ihm bei der Umsetzung ein gewisser Ermessensspielraum zu, bei dem auch mögliche Auswirkungen auf die internationalen Beziehungen der Bundesrepublik eine Rolle spielen.[18] Derzeit sieht es jedoch ganz danach aus, als wollte sich der Staat dieser Verantwortung entziehen. Daher werden vermutlich auch in diesem Falle die maßgeblichen Impulse von der Rechtsprechung des *BVerfG* ausgehen.[19] Auch wenn die Frage der technischen Realisierbarkeit und Wirksamkeit etwaiger

[13] Ähnlich *BVerfGE* 55, 349, 364; *BVerfGE* 66, 39, 61; *BVerfGE* 77, 170, 214 ff.; *Ewer/Thienel* NJW 2014, 30, 34.
[14] *Ewer/Thienel* NJW 2014, 30, 34.
[15] *BVerfG* NJW 1984, 419, 421.
[16] *Kipker/Voskamp* RDV 2014, 84, 85.
[17] *Kipker/Voskamp* RDV 2014, 84, 85.
[18] *BVerfG* NJW 1981, 1499; ähnlich *Ewer/Thienel* NJW 2014, 30, 34.
[19] Ähnlich *Hoffmann/Schulz/Borchers* MMR 2014, 89, 92.

Maßnahmen zweifelhaft erscheint[20], so sollte zumindest die Grenze des Untermaßverbots einen gewissen Anreiz zum Handeln geben. Seit nunmehr über einem Jahr ist nichts passiert. Weder Exekutive noch Legislative legen ein ernstzunehmendes Bemühen an den Tag. Offenbar bleibt dem Bürger damit mal wieder nichts anderes übrig, als auf eine Grundsatzentscheidung des *BVerfG* oder des *EGMR* zu hoffen.[21]

[20] Ähnlich *Kipker/Voskamp* RDV 2014, 84, 85.

[21] Neben dem Strafverfahren gegen die deutsche Bundesregierung hat der deutsche *Chaos Computer Club* (CCC) gemeinsam mit der britischen Organisation *Big Brother Watch* und dem Schriftstellerverband *PEN* Klage gegen die Überwachungspraxis des GHCQ beim *EGMR* eingereicht (vgl. Application No. 58170/13,
http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-140713.

3 Digitale Selbstverteidigung

Wer sich nicht auf staatliche Hilfe verlassen oder einfach nicht so lange warten will und über ein wenig technisches Verständnis verfügt, findet im World Wide Web eine Vielzahl von Anleitungen um seine Kommunikationsinhalte zu verschlüsseln und seine Spuren im Netz zu verschleiern.[22]

3.1 Technische Schutzmaßnahmen

3.1.1 Der Schutz von Kommunikationsinhalten

Das Verschlüsseln von Kommunikationsinhalten war noch nie so einfach wie heute. Viele kleine, europäische Anbieter von E-Mail-Diensten bieten neben der automatischen Verschlüsselung auf dem Transportweg und sicheren Verbindungen weitere Sicherheitseinstellungen, die sich ohne größeren Aufwand bedienen lassen.[23]

All diese Dienste haben jedoch einen entscheidenden Makel. Werden sie zu erfolgreich, sind sie nach § 110 TKG i.V.m. den Vorschriften der Telekommunikationsüberwachungsverordnung (TKÜV) verpflichtet, Ermittlungsbehörden und Nachrichtendiensten eine Schnittstelle zum automatischen Zugriff einzuräumen, was die Umgehung einer etwaigen anbieterseitigen Verschlüsselung mit einschließt. Die notwendige Erfolgsschwelle definiert der Gesetzgeber in § 3 Abs. 2 Nr. 5 TKÜV bei 10.000 Kunden. Die Amerikaner haben dagegen im US Patriot Act sowie dem Foreign Intelligence Surveillance Act (FISA) noch deutlich weitere rechtliche Grundlagen für eine systematische Überwachung ge-

[22] An dieser Stelle sei stellvertretend für viele auf die Anleitung des *Digitalcourage e.V.* verwiesen, https://digitalcourage.de/support/digitale-selbstverteidigung.
[23] Z. B. der E-Mail-Dienst Posteo, https://posteo.de/.

schaffen, Auskunftsansprüche gegenüber Internetserviceprovidern und eine gesonderte Gerichtsbarkeit, die sog. FISA-Courts, eingeschlossen. Dabei erfasst der Auskunftsanspruch auch Daten europäischer Bürger, selbst wenn diese ausschließlich von der europäischen Tochtergesellschaft eines amerikanischen Internetserviceproviders oder IT-Unternehmens erhoben, gespeichert und verarbeitet werden.[24]

In Sachen Verschlüsselung ist man jedoch nicht zwingend auf die Dienste anderer angewiesen. Mit wenig Aufwand und nicht allzu hohen Anforderungen an die eigenen technischen Kenntnisse lassen sich offene Verschlüsselungsstandards wie Open PGP einsetzen.[25] Quelloffene Formate setzen dabei vor allem auf Transparenz und lassen sich auf ihre Sicherheit und Authentizität hin überprüfen. Letztendlich lässt sich aber auch hier nicht gänzlich ausschließen, dass sich staatliche Sicherheitsbehörden über die Finanzierung derartiger Projekte auch einen gewissen Einfluss hierauf sichern. Auch hardwareseitige Verschlüsselungslösungen bieten hier keine weitreichendere Sicherheitsgarantien, da hier Hintertüren mitunter bereits in der Produktionsphase eingebaut werden[26] – sozusagen „Surveillance by Design“[27].

Neben den E-Mail-Diensten gibt es selbstvertändlich weitere Diensteanbieter und Programme, mit denen sich Kommunikationsinhalte, die über andere Kanäle (bspw. Voice over IP, Messenger etc.) ausgestauscht werden, verschlüsseln und vor dem unbefugten Zugriff Dritter schützen lassen.

---

[24] Vgl. auch *Ermert/Wilkens* Heise Online v. 21.2.2013, http://heise.de/-1807677.

[25] Das Format Open PGP basiert auf dem ursprünglichen von Phil Zimmermann entwickelten Programm PGP und dient der Verschlüsselung und digitalen Signatur von Daten. Die Abkürzung „PGP“ steht dabei für „Pretty good Privacy“.

[26] *Beiersmann* ZDNET v. 13.5.2014, http://www.zdnet.de/88192976/bericht-nsa-stattet-den-usa-hergestellte-hardware-mit-hintertueren-aus/.

[27] Als Gegenbegriff der im Bereich des Datenschutz vermehrt geforderten datenschutzfreundlichen Gestaltung / Produktion von (Software-) Produkten und Dienstleistungen („Privacy by Design“).

Die Begeisterung für die Nutzung sicherer bzw. verschlüsselter Kommunikationsalternativen wird allerdings in der Regel schnell erlahmen, wenn der Freundes- und Bekanntenkreis nicht mitzieht.

3.1.2 Anonymität im Internet

Im Gegensatz zu den Kommunikationsinhalten, die vor allem Gegenstand gezielter Überwachungsmaßnahmen im Einzelfalls sind, stehen bei der verdachtsunabhängigen, massenhaften Überwachung der Internetkommunikation vor allem die sog. „Meta-Daten" im Fokus. Diese im Kontext des Fernmeldegeheimnisses als nähere Umstände eines Telekommunikationsvorgangs bezeichneten Informationen unterliegen ebenso dem Schutzbereich des Art. 10 GG wie die eigentlichen Kommunikationsinhalte.[28] Informationen darüber, wer mit wem, wann und von wo, wie lange und mit welcher Regelmäßigkeit telefoniert, verschaffen bereits einen guten Überblick über das soziale Beziehungsgeflecht der Betroffenen. In Verbindung mit der Betreffzeile einer E-Mail, welche nicht mit verschlüsselt wird, lassen sich darüber hinaus inhaltliche Bezüge herstellen, ohne dass es hierzu der Kenntnis des eigentlichen (verschlüsselten) Inhalts bedürfte.

Das Verwischen seiner Spuren im Netz, etwa mithilfe des Anonymisierungsdienstes TOR (The Onion Router), macht, wie eine Quellcode-Analyse des Programms XKeyscore kürzlich gezeigt hat, in den Augen der NSA erst recht verdächtig.[29] Während die passive Nutzung dieses Anonymisierungsdienstes auf Peer-to-Peer-Basis (P2P) noch relativ gefahrlos möglich ist, kann der Betrieb eines TOR-Servers durchaus rechtliche Konsequenzen nach sich ziehen. Neben einigen größeren Serverstandorten basiert das TOR-Netzwerk überwiegend auf freiwillig von seinen Nutzern bereitgestellten Verbindungs- und

[28] *Durner* in: *Maunz/Dürig (Hrsg.)*, Grundgesetz-Kommentar, 2014, Art. 10, Rn. 81, 87; *Caspar* PinG 2014, 1, 3.
[29] *Holland,* Heise Online v. 3.7.2014, http://heise.de/-2248328.

Rechenkapazitäten. Die überwiegende Anzahl der TOR-Server wird folglich von Privatpersonen betrieben.

Während die technische Einrichtung eines solchen Servers selbst ohne größere technische Vorkenntnisse möglich ist, sind mit dem Betrieb doch vielfältige rechtliche Fragen und Risiken verknüpft. Rechtlich agiert der Betreiber eines TOR-Servers ähnlich einem Accessprovider, indem er dem Nutzer Zugang zu einem anonymisierten Sub-Netz innerhalb der Internetarchitektur gewährt und dessen Kommunikationssignale transportiert. Dabei handelt es sich bei Anonymisierungsdiensten um sog. hybride Dienste, die aufgrund ihrer Doppelnatur sowohl den Regelungen des Telekommunikationsgesetzes (TKG) als auch des Telemediengesetzes (TMG) unterfallen.[30] Damit finden die Vorschriften über die Haftungsprivilegierung nach § 7 ff. TMG grundsätzlich auch auf Anonymisierungsdienste Anwendung.

Ihre Betreiber haften somit grundsätzlich nicht für die von ihren Nutzern begangenen Rechtsverletzungen, sofern sie nicht kollusiv mit diesen zusammenwirken und nach Kenntniserlangung hinreichende und zumutbare Maßnahmen ergreifen, um noch andauernde bzw. künftige Verstöße zu unterbinden. Präventive Überwachungsmaßnahmen sind ihnen allerdings nicht zumutbar. Die Haftung ist zudem auf Beseitigungs- und Unterlassungsansprüche beschränkt, erfasst somit gerade nicht die Verpflichtung zur Zahlung von Schadensersatz. Dies gilt der nach wie vor h.M. zufolge allerdings nur für kommerzielle Dienste, nicht dagegen für private Anbieter.[31] Das Risiko für Rechtsverletzungen Dritter (bspw. Filesharing) zur Rechenschaft gezogen zu werden, dürfte beim privaten Betrieb eines TOR-Servers dabei ähnlich gelagert sein, wie beim Betrieb eines offenen Funknetzes (WLAN). Auch die rechtlichen Probleme, insbesondere im Hinblick auf Fragen der sog. Störerhaftung, sind weitest-

[30] Ausführlich zu dieser Problematik, *Rau/Behrens* K&R 2009, 766, 768.
[31] *BGH* ZUM 2010, 696, 698; krit. *Mantz* MMR 2010, 568, 570; *Brüggemann*, Der Drittauskunftsanspruch gegen Internetprovider, 2012, S. 95 ff.

gehend dieselben, auch wenn die Beurteilung der Sozialadäquanz beim Betrieb eines TOR-Servers anders ausfallen dürfte.

Weitaus gewichtiger sind die Konsequenzen im Bereich strafrechtlicher Ermittlungen. Es soll an dieser Stelle nicht verschwiegen werden, dass Anonymisierungsdienste wie das TOR-Netzwerk auch der Verschleierung krimineller Aktivitäten dienen. Der Vorwurf der Geldwäsche oder des Besitzes und der Verbreitung kinderpornografischen Materials und die oftmals damit einhergehende Hausdurchsuchung[32], dürften beim Betroffenen weitaus mehr Eindruck hinterlassen, obwohl er sich im Bezug auf die Beweislast in einer deutlich komfortableren Situation befindet als im Rahmen eines zivilrechtlichen Verfahrens zur Durchsetzung von Urheberrechtsansprüchen.

Andere Maßnahmen zur Gewährleistung von Anonymität (oder zumindest einer gewissen Datensparsamkeit) im Internet sind deutlich einfacher umzusetzen und mit deutlich weniger rechtlichen Risiken behaftet. Dazu gehört vor allem das Abschalten bestimmter Browser-Funktionen oder Plugins, die oftmals von Internetserviceprovidern und Werbetreibenden zum Nutzertracking verwandt werden.[33] Auf diese Weise werden zumindest einige zusätzliche Informationsquellen eliminiert, was indirekt die Arbeit der Geheimdienste erschwert.[34] Aber auch diese Maßnahme entpuppt sich schnell als zweischneidiges Schwert, lässt sich doch ein derart modifizierter Browser mittels der Methode des Browser-Fingerprintings deutlich leichter individualisieren.[35] Gleiches gilt für den Einsatz von Ad-Blockern.

---

[32] *Beckedahl,* Netzpolitik.org v. 17.5.2011, https://netzpolitik.org/2011/wieder-hausdurchsuchung-wegen-tor-exit-server/.
[33] Ausführlich zu den verschiedenen Tracking-Methoden, *Zeidler/Brüggemann* CR 2014, 248 ff.
[34] *Rosenblatt,* cnet v. 4.10.2013, http://www.cnet.com/news/nsa-tracks-google-ads-to-find-tor-users/.
[35] Vgl. *Zeidler/Brüggemann* CR 2014, 248 ff.

3.2 Digitale Formen des Protests

Fraglich ist, wie weit ein etwaiges Selbstverteidigungsrecht im digitalen Umfeld reicht und ob es neben rein passiven auch aktive Maßnahmen erfasst, wie bspw. Distributed-Denial-of-Service-Angriffe (DDoS) auf die technische Infrastruktur der Geheimdienste oder mit der Herstellung von Überwachungssoftware betrauter Unternehmen.

3.2.1 Virtuelle Demonstrationen

Die zunehmende Digitalisierung unsers Alltags betrifft auch unser Verhältnis zur Politik. Politischer Aktivismus und demokratische Auseinandersetzungen finden zunehmend im Internet statt.[36] Damit aber gewinnt die Frage nach der Anwendbarkeit der Grundsätze der Versammlungsfreiheit auf digitale Fallkonstellationen zunehmend an Dringlichkeit. Dies wurde bisher unter Verweis auf das Körperlichkeitserfordernis des Versammlungsbegriffs stets abgelehnt. Auf internationaler Ebene ist man hier dagegen schon deutlich weiter.[37]

Vorbereitungshandlungen im Vorfeld physischer Versammlungen über das Internet, bspw. die Verabredung und Organisation von Demonstrationen über Social Media-Kanäle oder den Kurznachrichtendienst Twitter unterfallen selbstverständlich dem Schutzbereich der Versammlungsfreiheit (Art. 8 GG), ebenso wie begleitende Formen der Dokumentation und Berichterstattung vor Ort. Mittels Videokonferenzen werden Redner oder Teilnehmer zugeschaltet oder umgekehrt die Versammlung übertragen, wobei das Internet als interaktives Medium grundsätzlich eine Kommunikation in beide Richtungen ermöglicht und somit integrativ wirkt. Folglich verschwimmen bereits heute die Grenzen

[36] So auch *Möhlers* MMR 2013, 221.

[37] So bspw. die Resolution des UN-Menschenrechtsausschusses (A/HRC/20/L.13 Promotion, protection and enjoyment of human rights on the Internet) aus dem Jahr 2012, die sich für einen Gleichlauf der Grund- und Menschenrechte offline wie online ausspricht.

zwischen der körperlichen Versammlung vor Ort und den über das Internet zugeschalteten Teilnehmern.[38] Warum also sollten nicht auch rein virtuelle Versammlungen dem Schutz des Art. 8 GG unterstehen?

Distributed-Denial-of-Service-Attacken (DDoS) wurden bereits in der Vergangeheit als Form des politischen Protests eingesetzt. So beispielsweise im Jahr 2010, als verschiedene Kreditkartenfirmen sowie der Online-Bezahldienst Paypal die Weiterleitung von Zahlungen an die Betreiber der Enthüllungsplattform Wikileaks verweigerten und die entsprechenden Spendengelder einfroren. Als Reaktion hierauf eröffneten weltweit einige tausend Nutzer mittels des als „Ionenkanone" bezeichneten Programms das virtuelle Feuer auf die Server der Dienste und legten diese für einige Tage lahm. Der Aufruf zu dieser als „Operation Payback" bezeichneten „Protestaktion" stammte aus dem Umfeld der Protestbewegung „Anonymous".[39] Das Prinzip hinter einer „DoS"-Attacke ist dabei denkbar einfach. Mittels eines Computerprogramms wird eine dauerhaft hohe Anzahl von Zugriffe auf die Webseite eines Unternehmens ausgelöst, bis diese unter der Last der Anfragen zusammenbrechen und für andere Kunden nicht mehr erreichbar sind. Werden solche Angriffe in Absprache mit mehreren Beteiligten oder, wie im kriminellen Umfeld üblich, unter Rückgriff auf ein Bot-Netz ausgeführt, sprich man von einem koordinierten Angriff und somit einer „Distributed-Denial-of-Service"-Attacke (DDoS). Diese Form des Protests wird mitunter auch als virtuelle Sitzblockade bezeichnet.[40]

Bei einer Versammlung handelt es sich nach landläufiger Auffassung um eine bewusste, friedliche Zusammenkunft mehrerer Personen zur Verfolgung eines gemeinsamen Zwecks.[41] Das Merkmal der Personenmehrheit dürfte dabei

---

[38] Ähnlich *Möhlers* MMR 2013, 221, 223.
[39] Vgl. *Patalong,* Spiegel Online v. 9.12.2010, http://www.spiegel.de/netzwelt/web/rache-fuer-wikileaks-dauerfeuer-aus-ionenkanonen-a-733703.html.
[40] *Kraft/Meiser* K&R 2005, 366; *Klutzny* RDV 2006, 50; *Möhlers* MMR 2013, 221, 223.
[41] *Mann/Ripke* EuGRZ 2004, 125, 127; *Möhlers* MMR 2013, 221, 223.

regelmäßig erfüllt sein, sieht man einmal von dem Fall ab, in dem der Angriff durch ein Bot-Netz erfolgt.

Ähnlich dem Postkartenprotest wissen die Teilnehmer untereinander in der Regel nichts von einander und handeln mangels Absprache nicht koordiniert und ohne die Möglichkeit sich untereinander auszutauschen, weshalb es am Merkmal der Zusammenkunft fehlen könnte. Auch für Außenstehende, ist das Zusammenwirken zumeist nicht eindeutig erkennbar.[42] Dieses Manko ließe sich allerdings auf technischem Wege beheben, bspw. indem man die Ionen-Kanone um ein Chatprogramm erweitert.

Problematisch sind neben der Frage der Körperlichkeit ferner auch die der Verfolgung eines gemeinsamen Zwecks sowie die der Friedlichkeit. Bei der gemeinsamen Zweckverfolgung wird es in der Regel an der äußerlichen Erkennbarkeit fehlen. Lässt sie sich der DDoS-Attacke selbst nicht entnehmen, ließe sie sich aber in Form einer entsprechenden medialen Ankündigung ausdrücken. Auch fehlt es nicht bereits an der Friedlichkeit, nur weil durch die Aktion der Zugriff auf das betroffene Webangebot blockiert ist. Dies ist auch im Falle der herkömmlichen Sitzblockade der Fall, ohne dass es allein deshalb an der Friedlichkeit der Veranstaltung fehlte. Ob der Vergleich zwischen passiver Offline-Präsenz und dem massenhaften, aktiven Abruf einer Webseite tatsächlich noch vergleichbar sind, darf zwar bezweifelt werden.[43] Beeinträchtigt wird letztendlich jedoch lediglich die Erreichbarkeit des Angebots, lediglich die Intensität der eigenen, virtuellen Präsenz wird mit technischen Mitteln gesteigert. Im Ergebnis spricht daher vieles dafür, dass eine DDoS-Attacke, entgegen ihrer Bezeichnung, noch nicht die Schwelle zur Unfriedlichkeit überschreitet.[44] Vom Merkmal der Körperlichkeit abgesehen, bestünde unter bestimmten Umständen somit tatsächlich die Möglichkeit eine DDoS-Attacke als vom

[42] So *Möhlers* MMR 2013, 221, 224.
[43] *Kraft/Meiser* K&R 2005, 366, 368; *Klutzny* RDV 2006, 50, 52 f.
[44] So auch *Möhlers* MMR 2013, 221, 227.

Grundrecht auf Versammlungsfreiheit gedeckt anzusehen.[45] Auf die Mehrzahl der bisher bekannten Fälle dürfte dies dagegen nicht zutreffen.

3.2.2 Der "Hackback" als Form der Notwehr

Fraglich ist ebenfalls, ob sich auch ein, ansonsten nach § 202c StGB strafbares, Eindringen in die Computersysteme der Geheimdienste oder mit der Herstellung von Überwachungssoftware betrauter Unternehmen vor dem Hintergrund der NSA-Affäre nach § 34 StGB bzw. aufgrund einer (übergesetzlichen) Notstandslage rechtfertigen oder zumindest entschuldigen ließe.

Dass es sich hierbei keineswegs um ein rein theoretisches Gedankenspiel handelt, zeigt der jüngste Hack der Server des deutsch-britischen Unternehmens *Gamma International* mit Sitz in München, dass sich auf die Herstellung von Überwachungssoftware (u.a. dem Staatstrojaner) spezialisiert hat und diese Technik auch in totalitäre Regime exportiert.[46] Dabei hatte der Hacker Dokumente erbeutet, die belegen, dass das Unternehmen für die Überwachungssoftware FinFisher einen Wartungsvertrag mit dem Staat Bahrain geschlossen hat. Die vorangegangene Erklärung des Unternehmens, die Software sei Ihnen auf einer Messe gestohlen worden,[47] dürfte damit hinfällig sein.

Aufgrund der eher diffusen Betroffenheitssituation dürfte es sich sowohl im Hinblick auf die Tätigkeit der Geheimdienste als auch auf die Hersteller von Überwachungssoftware als schwierig erweisen, vom Vorliegen einer Notwehrlage auszugehen. Die anlasslose Massenüberwachung durch NSA und GHCQ dürfte wohl einen gegenwärtigen, rechtswidrigen Angriff begründen, bei dem jedoch nicht erkennbar ist, gegen wen er sich nun im konkreten Fall richtet. Zwar käme hier grundsätzlich auch eine Form der Nothilfe in Betracht, aller-

[45] A.A. *Möhlers* MMR 2013, 221, 226.
[46] Vgl. *Borchers/Benz* Heise Online v. 9.8.2014, http://heise.de/-2289532.
[47] Vgl. *Opitz,* Heise Online v. 9.2.2013, http://heise.de/-1801126.

dings dürfte es auch hier schwierig werden einen konkreten Bezugspunkt für die Bildung eines Verteidigungswillens auszumachen.

Im oben genannten Beispiel steht die bezweckte Informationsbeschaffung zudem in keinem unmittelbaren Zusammenhang zu einem gegenwärtig stattfindenden Angriff, selbst dann, wenn das Regime in Bahrain die Software in diesem Moment eingesetzt hat. In jedem Fall scheitert die Notwehr in diesem Fall daran, dass sie sich nicht gegen die Rechtsgüter des Angreifers, sondern gegen die eines, wenn auch nicht gänzlich unbeteiligten, Dritten richtet. Eine Rechtfertigung durch Notwehr (§ 32 StGB) scheidet folglich aus.

Im vorgenannten Beispiel scheidet aber auch eine Rechtfertigung nach § 34 StGB aus, da die Tat zwar der Aufklärung des Sachverhalts, nicht aber der Abwehr einer Gefahr bzw. der Verhinderung künftiger Angriffe diente. Im Falle der Massenüberwachung durch (ausländische) Geheimdienste, wird man gleichwohl von einer gegenwärtigen Dauergefahr ausgehen müssen. Das bedrohte Rechtsgut sind in diesem Falle die betroffenen Grundrechtspositionen. Die Frage der Güterabwägung bleibt letztendlich der Entscheidung im Einzelfall vorbehalten, dürfte aufgrund der Schwere des Eingriffs aber grundsätzlich eine Tendenz zugunsten des Notstandshandelnden aufweisen.

Angesichts des Ausmaßes der Affäre und der diffusen Betroffenheitssituation, die sich auf das Verhältnis von Gefährdung und Verteidigungshandlung, Aktion und Reaktion auswirkt, drängt sich hier allerdings förmlich die Frage auf, ob der Beurteilungsmaßstab des Strafrechts tatsächlich noch geeignet ist, den Sachverhalt in Gänze zu erfassen. Vor diesem Hintergrund liegt es nahe, zur Beseitigung der Notstandslage vorranging auf die Hilfe der Staatsgewalt zu setzen, allein sie lässt sich bitten.

3.3 Das Widerstandsrecht als ultima ratio

Dies bedeutet in letzter Konsequenz aber auch darüber nachzudenken, ob in dieser Situation nicht das in der Verfassung verankerte Widerstandsrecht des Art. 20 Abs. 4 GG – ultima ratio – greifen könnte.

Der vormalige Bundesdatenschutzbeauftragte *Thilo Weichert* hat, im Zusammenhang mit der Weiterentwicklung der verfassungsrechtlichen Grundlagen des Datenschutzrechts und damit des Rechts auf informationelle Selbstbestimmung, dem Recht zur Selbsthilfe bzw. Selbstverteidigung, angesichts „der informationstechnischen dauernden und situationsunabhängigen Gefährdungslage", wesentliche Bedeutung beigemessen und sich für eine umfassendere Interpretation ausgesprochen.[48] Dies gilt heute umso mehr wie damals. Freilich hatte *Weichert* seinerzeit weder die vorstehend diskutierten Protest- und Verteidigungshandlungen noch das Widerstandsrecht des Grundgesetzes im Auge. Sein Recht auf Selbstverteidigung zielte seinerzeit vor allem auf die Möglichkeiten eines informationstechnischen Identitätsmanagements, das seiner Auffassung nach vor allem in einem Recht auf Verschlüsselung und Anonymität besteht und somit im wesentlichen die vorstehend diskutierten Möglichkeiten des (passiven) technischen Selbstschutzes umfasst.[49]

Beim positivierten Widerstandsrecht des Art. 20 Abs. 4 GG handelt es sich dagegen um *„eine der dogmatisch interessantesten, zugleich aber auch bedenklichsten Bestimmungen"* des Grundgesetzes.[50] Dem Wortlaut nach zufolge hat jeder Deutsche ein Recht zum Widerstand gegen jeden, der es unternimmt, die in den voranstehenden Absätzen konkretisierte Ordnung unseres Staates zu beseitigen. Das Widerstandsrecht gilt allerdings nicht unbeschränkt, sondern

---

[48] *Weichert,* in: *Kilian/Heussen* (Hrsg.), Computerrechts-Handbuch, 2008, Teil 13, Rn. 43.
[49] Vgl. *Weichert,* in: *Kilian/Heussen* (Fn. 48), Teil 13, Rn. 43.
[50] So *Herzog/Grzeszick* in: *Maunz/Dürig* (Fn. 28), Art. 20, Kap. IX, Rn. 1.

unter dem Vorbehalt, dass anderweitige Abhilfe nicht möglich ist. Historisch gesehen, stellt das Widerstandsrecht eine unmittelbare Reaktion auf die Notstandsverfassung des Dritten Reichs dar. Vor diesem Hintergrund richtet sie sich in erster Linie gegen einen *„Staatsstreich von oben"*.[51] Handlungen im Rahmen des bestehenden und an sich noch unkorrumpierten politischen Systems, die sich ausschließlich gegen bestimmte hoheitliche Maßnahmen, wie etwa die Tätigkeit der inländischen Nachrichtendienste richten, waren nie intendiert, geschweige denn Handlungen, die sich gegen andere Staaten richten. Das Widerstandsrecht ist Grundrecht, weist aber gleichzeitig einen staats- und verfassungsschutzrechtlichen Charakter auf.[52] So gesehen handelt es sich um die einzige Sanktion der Verfassungsordnung – außerhalb des Strafrechts – und begründet eine Form des inneren Verfassungsnotstands, in dem die Sanktionen des politischen Strafrechts nicht mehr ausreichen bzw. versagt haben und keine Bereitschaft mehr besteht sich der Autorität des *BVerfG* zu beugen.[53] Von dem hier beschriebenen, innerdeutschen Bürgerkriegsszenario sind wir tatsächlich noch ein Gutes Stück entfernt, auch wenn es keinen Anlass dazu gibt, die grundsätzliche Bedrohung unserer freiheitlichen Demokratischen Grundordnung durch die anlasslose Massenüberwachung (ausländischer) Geheimdienste zu verharmlosen. Gegen die Untätigkeit von Exekutive und Legislative steht dem Bürger in unserem nach wie vor funktionierenden System der Rechtsweg und in letzter Instanz der Weg zum *BVerfG* offen, der auch, wie zuvor aufgezeigt, bereits beschritten wurde. Zumindest vorerst bleibt uns daher nichts anderes übrig, als abzuwarten und die Möglichkeiten des digitalen Selbstschutzes sowie die zulässigen Formen des politischen Protests auszuschöpfen.

[51] So *Herzog/Grzeszick,* in: *Maunz/Dürig* (Fn. 28), Art. 20, Kap. IX, Rn. 2.
[52] So *Herzog/Grzeszick,* in: *Maunz/Dürig* (Fn. 28), Art. 20, Kap. IX, Rn. 5.
[53] So *Herzog/Grzeszick,* in: *Maunz/Dürig* (Fn. 28), Art. 20, Kap. IX, Rn. 5.

4 Fazit

Die diffuse Grundrechtsbetroffenheit des Einzelnen im Rahmen der NSA-Affäre und die trotz der zahlreichen Enthüllungen nach wie vor weitgehend ungesicherte Tatsachenbasis, erschweren die rechtliche Aufarbeitung der Affäre seitens der Gerichte. Gleichzeitig scheinen Exekutive und Legislative nicht gewillt oder sind schlicht nicht in der Lage, an den bestehenden Zuständen etwas zu ändern. Ob wir tatsächlich bereits in *„postdemokratischen Zuständen"* leben, wie es der Schriftsteller *Hans Magnus Enzensberger* in einem Fernsehinterview kurz nach Bekanntwerden der NSA-Affäre im Jahr 2013 beschrieb,[54] darf bezweifelt werden. Die Richtung haben wir jedenfalls längst eingeschlagen.

Der bisherige Verlauf der NSA-Affäre lässt jedoch bereits erahnen, dass sich am derzeitigen Zustand so schnell nichts ändern wird. Dem betroffenen Bürger bleibt damit vorerst nichts anderes übrig, als seinen Grundrechten selbst auf technischem Wege Geltung und sich selbst durch zulässige Formen des politischen Protests Gehör zu verschaffen. Wie weit das Recht auf digitale Selbstverteidigung auch strafrechtlich relevante Handlungen, wie etwa das Eindringen in fremde Computersysteme und die Beschaffung von zur Aufklärung notwendigen Informationen umfasst, hängt stets maßgeblich von den Umständen des Einzelfalls ab. Umso wichtiger ist es, einen effektiven Quellenschutz im journalistischen Bereich zu wahren. Auch der Rechtsweg steht nach wie vor offen. Wer nach alldem jedoch nach wie vor der Auffassung ist, all dies ginge ihn nichts an, denn schließlich habe er nichts zu verbergen, hat seine Grundrechte bereits abgeschrieben.

---

[54] Vgl. *Weidermann,* FAZ Online v. 19.8.2013, http://www.faz.net/aktuell/feuilleton/medien/tv-kritik/in-der-ard-enzensberger-zu-snowden-ein-held-des-21-jahrhunderts-12537881.html.

Autorenhinweise

Prof. Dr. Kai von Lewinski ist seit Beginn des Sommersemesters 2014 Professor an der Juristischen Fakultät der Universität Passau. Zuvor war er Wissenschaftlicher Leiter der Stiftung Datenschutz und Lehrstuhlvertreter an verschiedenen Universitäten, darunter an der HU Berlin und am Karlsruhe Institut für Technologie (KIT); davor Rechtanwalt in einer internationalen Wirtschaftskanzlei mit Arbeitsschwerpunkten im Datenschutz- und Softwarelizenzrecht. Kai von Lewinski arbeitet u.a. zum Datenschutzrecht und zu Big Data.

Simon Assion ist Redakteur bei Telemedicus. Außerdem Juristischer Referent beim Mitteldeutschen Rundfunk, Promotionsstudent am Hans Bredow-Institut in Hamburg und Sprecher der Landesarbeitsgemeinschaft Medien- und Netzpolitik von Bündnis 90/Die Grünen in Sachsen.

Jakob Dalby studierte Rechtswissenschaften an der WWU Münster, Zusatzausbildung Informations-, Telekommunikations- und Medienrecht, Dipl. Jur., gegenwärtig Referendar am OLG Celle sowie wissenschaftliche Hilfskraft an der Deutschen Hochschule der Polizei im Fachgebiet Öffentliches Recht mit Schwerpunkt Polizeirecht einschließlich des internationalen Rechts und des Europarechts. Forschungsschwerpunkt Strafverfolgung im Internet und Zugriff auf Cloud-Speicher.

Philipp Wunderlin ist seit 2012 Rechtsanwalt bei Härting Rechtsanwälte. Nach seinem Studium in München und Köln machte er einen Master an der Victoria University in Wellington, Neuseeland. Sein Referendariat absolvierte er am Kammergericht Berlin. Bei Härting Rechtsanwälte ist Philipp Wunderlin für die Betreuung von Start-Ups zuständig.

Dipl.-Inf. Dipl.-Jur. Agata Królikowski hat an der Humboldt-Universität zu Berlin Jura und Informatik studiert. Zur Zeit ist sie wissenschaftliche Mitarbeiterin am Innovations-Inkubator der Leuphana Universität Lüneburg und arbeitet dort in den Projekten Hybrid Publishing und Grundversorgung 2.0. Daneben ist sie Präsidiumsmitglied und Mitglied des erweiterten Vorstands der Gesellschaft für Informatik e.V. sowie Sprecherin der Fachgruppe Internet und Gesellschaft.

Dr. Sebastian Brüggemann, M.A. berät als Rechtsanwalt seit 2013 nationale und internationale Unternehmen sowie Kreativschaffende in Fragen des Urheber-, Medien-, IT- und Datenschutzrechts zunächst im Stuttgarter Büro der Sozietät SGT Rechtsanwälte, seit 2014 im Team Technologie Medien Telekommunikation bei PwC Legal am Standort Düsseldorf. Parallel zu seiner Promotion zu einem urheber- und informationsrechtlichen Thema absolvierte er sein Referendariat, in einer auf Urheber- und IT-Recht spezialisierten Kanzlei sowie beim Verband der deutschen Internetwirtschaft e.V. (eco) in Köln. Er ist Autor zahlreicher Fachbeiträge (u.a. auch bei Telemedicus) und engagiert sich auch privat in Sachen Netzpolitik. Seit 2013 betreut er zudem einen Lehrauftrag (Internetrecht) an der Juristischen Fakultät der Eberhard Karls Universität Tübingen.