Policy Paper

Rechtsschutz im Staatsschutz?

Das Menschenrecht auf wirksame Beschwerde in der Terrorismus- und Extremismusbekämpfung

Eric Töpfer

Deutsches Institut
für Menschenrechte

Impressum

Deutsches Institut für Menschenrechte

Zimmerstr. 26/27
10 969 Berlin
Tel.: 030 25 93 59–0
Fax: 030 25 93 59–59
info@institut-fuer-menschenrechte. de
www. institut-fuer-menschenrechte. de

Satz:
Da-TeX Gerd Blumenstein, Leipzig

Druck:
dieUmweltDruckerei, Langenhagen

Policy Paper Nr. 33
September 2015

ISBN 978-3-945-139-73-8 (PDF)
ISBN 978-3-945-139-74-5 (Print)

ISSN 1614-2195 (PDF)
ISSN 1614-2187 (Print)

Der Autor

Eric Töpfer ist wissenschaftlicher Mitarbeiter am Deutschen Institut für Menschenrechte. Seine Arbeitsschwerpunkte sind Menschenrechte im Feld der Inneren Sicherheit und Datenschutz. Außerdem ist er zuständig für die sozialwissenschaftliche Berichterstattung an die Agentur der Europäischen Union für Grundrechte.

Das Institut

Das **Deutsche Institut für Menschenrechte** ist die unabhängige Nationale Menschenrechtsinstitution Deutschlands. Es ist gemäß den Pariser Prinzipien der Vereinten Nationen akkreditiert (A-Status). Zu den Aufgaben des Instituts gehören Politikberatung, Menschenrechtsbildung, Information und Dokumentation, angewandte Forschung zu menschenrechtlichen Themen sowie die Zusammenarbeit mit internationalen Organisationen. Das Institut wird vom Bundesministerium der Justiz und für Verbraucherschutz, vom Auswärtigen Amt und von den Bundesministerien für wirtschaftliche Zusammenarbeit und Entwicklung sowie für Arbeit und Soziales gefördert. Im Mai 2009 wurde die Monitoring-Stelle zur UN-Behindertenrechtskonvention im Institut eingerichtet.

Zusammenfassung

Jeder Mensch hat das Recht auf wirksame Beschwerde, um sich gegen mutmaßliche Verletzungen seiner Menschenrechte zu wehren. Im Feld der Terrorismus- und Extremismusbekämpfung ist dieses Recht jedoch besonders herausgefordert, da Geheimhaltung dominiert und Betroffene nur schwer oder gar nicht Kenntnis über Eingriffe in ihre Rechte erhalten. Wie ist es angesichts dessen um den Rechtsschutz im Staatsschutz bestellt?

Das vorliegende Policy Paper geht dieser Frage in drei Schritten nach: In einem kurzen Abriss wird das Feld grund- und menschenrechtlicher Verpflichtungen abgesteckt, in dem sich das Menschenrecht auf wirksame Beschwerde in der Terrorismus- und Extremismusbekämpfung bewegt. Anschließend werden rechtliche und praktische Probleme dargestellt, die sich bei der Umsetzung der menschenrechtlichen Verpflichtungen in Deutschland stellen. Abschließend werden die aufgezeigten Defizite erörtert und Empfehlungen zur Stärkung des individuellen Rechtsschutzes und der Kontrolle von Sicherheitsbehörden formuliert.

Inhalt

Rechtsschutz im Staatsschutz?

Das Menschenrecht auf wirksame Beschwerde in der Terrorismus- und Extremismusbekämpfung

1 Einleitung

Seit die Novellierung der Gesetze zur Antiterrordatei (ATD) und Rechtsextremismusdatei (RED) am 1. Januar 2015 in Kraft trat, braucht es für Projekte, mit denen eine Sicherheitsbehörde des Bundes Daten aus einer der beiden Dateien nutzen will, um Beziehungsnetzwerke, Reisebewegungen oder statistische Auffälligkeiten zu analysieren, die Zustimmung der G 10-Kommission.[1] Die Kommission war 1968 durch das Artikel 10-Gesetz (G 10) ins Leben gerufen worden, um die Post- und Fernmeldeüberwachung durch die bundesdeutschen Nachrichtendienste gerichtsähnlich zu kontrollieren. Mit der neuen Aufgabe wurde der Kommission nun erstmals die Kompetenz übertragen, in – wie üblich – geheimen Verfahren auch über die Legalität polizeilicher Maßnahmen zu entscheiden. Obwohl dieses kleine, aber bemerkenswerte Detail im Gesetzgebungsverfahren 2014 kaum Beachtung fand, illustriert es mit aller Deutlichkeit, dass das Feld der Terrorismus- und Extremismusbekämpfung[2] in wachsendem Maße von Geheimhaltung durchdrungen wird.

Angesichts dieser Entwicklung wird schon seit längerem von einer „Vergeheimdienstlichung" beziehungsweise „Vernachrichtendienstlichung" von Strafverfolgung und Gefahrenabwehr gesprochen.

Gemeint ist damit zum einen der Bedeutungszuwachs, den nachrichtendienstliche Informationen für die Arbeit von Staatsanwaltschaft, Polizei und verwandten Ordnungsbehörden erlangt haben. Dabei kann es um die Initiierung polizeilicher Maßnahmen durch nachrichtendienstlich veranlasste Ausschreibungen zur (grenz-)polizeilichen Beobachtung gehen,[3] um die ordnungsbehördliche Konsultation von Nachrichtendiensten, wie sie zum Beispiel bei Zuverlässigkeitsüberprüfungen[4] oder bei aufenthaltsrechtlichen „Gefährder"-Analysen[5] stattfindet, oder auch um die Übermittlung von Informationen durch die Nachrichtendienste für die Verhinderung oder Verfolgung von Staatsschutzdelikten oder sonstige Zwecke der öffentlichen Sicherheit.[6] Neu ist die Kooperation zwischen Nachrichtendiensten und anderen Behörden nicht. Allerdings hat sie im Zeichen des neuen Paradigmas der „vernetzten Sicherheit" erheblich an Bedeutung gewonnen. So werden durch das Staatsschutz-Strafrecht in wachsendem Maße auch Vorbereitungshandlungen kriminalisiert, deren Ausforschung auf nachrichtendienstliche Erkenntnisse angewiesen ist. Außerdem wurde der Kreis der Einrichtungen und Objekte, die als sicherheitsrelevant gelten, in den letzten Jahren deutlich erweitert – entsprechend ist der Umfang von Sicherheits- und Zuverlässigkeitsüberprüfungen gestiegen.[7] Und nicht zuletzt wurde mit der Einrichtung

1 § 6a Abs. 8 ATD-Gesetz bzw. § 7 Abs. 8 RED-Gesetz.
2 Sowohl „Terrorismus" als auch „Extremismus" sind umstrittene, politisch umkämpfte und entsprechend unscharfe Begriffe, gleichwohl werden sie hier der Einfachheit halber genutzt, um die Gegenstände des Handelns von (polizeilichem) Staats- und (nachrichtendienstlichem) Verfassungsschutz zu markieren.
3 § 17 Abs. 2 bzw. Abs. 3 Bundesverfassungsschutzgesetz (BVerfSchG) i. V. m. § 31 Abs. 7 Bundespolizeigesetz (BPolG) bzw. Art. 36 EU-Ratsbeschluss 2007/533/JI zum SIS II i. V. m. § 17 Abs. 3 BVerfSchG.
4 Siehe u. a. § 12b Atomgesetz; § 7 Luftsicherheitsgesetz; § 34a Gewerbeordnung i. V. m § 9 Verordnung über das Bewachungsgewerbe.
5 §§ 54 ff. sowie §§ 72a ff. Aufenthaltsgesetz.
6 Siehe insbesondere §§ 19 und 20 BVerfSchG.
7 Ein Indikator hierfür ist der Zuwachs der aufgrund von Sicherheits- und Zuverlässigkeitsüberprüfungen im nachrichtendienstlichen Informationssystem (NADIS) erfassten Personen, der sich von 2001 bis 2014 fast verdreifacht hat und von 499.000 auf 1.376.123 anstieg. Vgl. Bundesministerium des Innern (Hg.) (2002): Verfassungsschutzbericht 2001, Berlin, S. 11 und Bundesministerium des Innern (Hg.) (2015): Verfassungsschutzbericht 2014, Berlin, S. 14.

gemeinsamer Zentren und Dateien seit 2004 ein alltäglicher und automatisierter Informationsaustausch zwischen Behörden mit eigentlich sehr unterschiedlichen Aufgaben institutionalisiert, wie er zuvor nicht vorstellbar war.[8]

Zum anderen meint der Begriff „Vernachrichtendienstlichung" die wachsende Ausstattung von Strafverfolgung und Polizei mit Kompetenzen und Instrumenten zur heimlichen Informationserhebung. Beispiele hierfür sind Verdeckte Ermittler, V-Leute, „Lausch- und Spähangriffe" und die Überwachung von Telekommunikation. Hinzu kommen komplexe und – immer mehr auch – organisations- und grenzübergreifende Formen der Datenverarbeitung wie etwa die „Rasterfahndung" oder eben die eingangs genannten Analyseprojekte zur Auswertung großer Datenbestände aus unterschiedlichsten Quellen.

Auch wenn die verdeckten Methoden heute in unterschiedlichsten Bereichen zum Einsatz kommen, so waren Staatsschutz und Terrorismusbekämpfung in der Regel das Feld, in dem ihre Anwendung zuerst erprobt wurde.[9] Unabhängig vom Einsatzbereich lässt sich jedoch konstatieren, dass der „Zweck dieser Vorgehensweise […] dabei weniger [ist], gerichtsverwertbare, beweiserhebliche Informationen zu erlangen, sondern allgemeine kriminalstrategische Ziele durch Erkenntnisgewinn im und über das ‚Milieu' zu erreichen".[10]

Legimitiert wird diese Entwicklung mit dem Verweis auf Bedrohungen durch mehr oder weniger abstrakte Gefahren, kaum kalkulierbare Risiken in einer global und digital vernetzten Welt, in welcher Ereignisse und Handlungen auch weit jenseits territorialer Grenzen und unmittelbarer Rechtsgüterschädigung im Ergebnis verheerende Auswirkungen haben können – ähnlich wie die vermeintlich unschuldigen Flügelschläge eines Schmetterlings in Asien, die – in der Metapher der Chaosforschung – einen verheerenden Sturm in Europa auslösen. Geboten sei daher die Abkehr sowohl von klassischen Methoden der strafprozessualen Verdachtsschöpfung als auch von der gefahrenabwehrrechtlichen „Störer"-Dogmatik zugunsten eines Programms der vorbeugenden Bekämpfung von Straftaten.

Was bedeutet es für die Menschenrechte, wenn heimliche Maßnahmen und geheime Informationen bei der Bekämpfung von Terrorismus und Extremismus in wachsendem Maße staatliches Handeln prägen? Eine verdeckte Überwachung greift – wenngleich nicht spürbar – in erheblichem Maße in das Recht auf Privatsphäre (Art. 17 Zivilpakt und Art. 8 EMRK) ein. Gleiches gilt, wenn personenbezogene Daten im Rahmen von Sicherheitskooperationen an Drittstaaten weitergeben werden. Diese Datenweitergabe birgt das Risiko gravierender Folgen: Geraten Informationen in die falschen Hände, kann es in den „schmutzigen Kriegen" des globalen Antiterrorkampfes zu Verstößen gegen das Recht auf Leben (Art. 6 Zivilpakt und Art. 2 EMRK) oder das Folter- und Misshandlungsverbot (Art. 7 Zivilpakt und Art. 3 EMRK) kommen. Wer aufgrund von Erkenntnissen des Staatsschutzes als „Gefährder" mit aufenthaltsrechtlichen Meldeauflagen, einer Ausweisung oder einem Ausreiseverbot belegt wird, dessen Bewegungs- und Reisefreiheit (Art. 12 Zivilpakt) ist beschnitten. Wem bei einer Zuverlässigkeitsüberprüfung Verfassungsfeindlichkeit unterstellt wird, dessen freie Berufswahl (Art. 6 Sozialpakt) kann in Frage stehen. Wenn aufgrund vertraulicher Terrorwarnungen eine Demonstration untersagt wird, so bedeutet das einen Eingriff in das Versammlungsrecht (Art. 21 Zivilpakt und Art. 11 EMRK). Werden Menschen heimlich beim Besuch des Freitagsgebetes registriert, ist dies ein Eingriff in ihre Religionsfreiheit (Art. 19 Zivilpakt und Art. 20 EMRK). Und wer staatlich sanktioniert wird, ohne die Gründe hierfür zu kennen, dessen Recht auf ein faires Verfahren (Art. 14 Zivilpakt und Art. 6 EMRK) ist beschnitten.

8 Allein in den vier großen gemeinsamen Zentren (das Gemeinsame Terrorismusabwehrzentrum mit dem Gemeinsamen Internetzentrum – GTAZ/GIZ, das Gemeinsame Analyse- und Strategiezentrum illegale Migration – GASIM, das Nationale Cyberabwehrzentrum – NCAZ und das Gemeinsame Extremismus- und Terrorismusabwehrzentrum mit dem Abwehrzentrum gegen Rechtsextremismus – GETZ/GAR) kommen mehr als 500 Bedienstete aus Sicherheitsbehörden von Bund und Ländern zum Teil täglich zu Lagebesprechungen zusammen. Siehe die Zusammenstellung bei Töpfer, Eric (2013): Informationsaustausch zwischen Polizei und Nachrichtendiensten strikt begrenzen. Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei. Berlin: Deutsches Institut für Menschenrechte (Policy Paper 21), S. 7. Zudem waren 2013 – vor der Bereinigung nach dem ATDG-Urteil des Bundesverfassungsgerichts – etwa 30. 000 Personen in den beiden Gemeinsamen Dateien ATD und RED erfasst, die gemeinsam von Polizei, Nachrichtendiensten und anderen Sicherheitsbehörden betrieben werden. Vgl. Deutscher Bundestag (2013): Bericht zur Evaluierung des Antiterrordateigesetzes. Unterrichtung durch die Bundesregierung. Drucksache 17/12 665, 07.03.2013, S. 5 sowie Deutscher Bundestag (2013): Polizeiliche Datensysteme zur Erfassung und Analyse Politisch motivierter Kriminalität – rechts. Antwort der Bundesregierung auf eine Kleine Anfrage, S. 2.

9 Pütter, Norbert (2012): Kontrollprobleme neuen Ausmaßes. Polizeilicher Staatsschutz als Geheimpolizei. In: Bürgerrechte & Polizei/CILIP (Heft 103), S. 11–22 (14 ff.).

10 Hefendehl, Roland (2011): Die Entfesselung des Strafverfahrens über Methoden der Nachrichtendienste. Bestandsaufnahme und Rückführungsversuch. In: Goltdammer's Archiv für Strafrecht, S. 209–231 (216).

Viele der genannten Rechte sind nicht absolut und dürfen aus Gründen der öffentlichen oder nationalen Sicherheit eingeschränkt werden. Allerdings stellt sich im Zeichen der neuen Heimlichkeit die drängende Frage, welche Möglichkeiten zur Überprüfung und Korrektur Betroffene haben, falls ihre Rechte zu Unrecht beschnitten werden. Wie kann das Recht auf wirksame Beschwerde (Art. 2 Abs. 3 Zivilpakt und Art. 13 EMRK) – der individuelle Rechtsschutz – in der Terrorismus- und Extremismusbekämpfung wahrgenommen werden, einem Bereich, in dem exekutives Handeln maßgeblich durch klandestin agierende Sicherheitsbehörden geprägt ist?

Dieser Frage wird im Folgenden in drei Schritten nachgegangen: Zuerst wird in einem kurzen Abriss das Feld grund- und menschenrechtlicher Verpflichtung abgesteckt, in dem sich das Gebot der Rechtsschutzgarantie im Bereich des Staatsschutzes bewegt. Anschließend werden schlaglichtartig rechtliche und praktische Probleme dargestellt, die sich bei der Umsetzung der menschenrechtlichen Verpflichtungen stellen. Abschließend werden die aufgezeigten Defizite erörtert und Empfehlungen formuliert. Im Sinne der Übersichtlichkeit ist dabei Vereinfachung geboten: Daher beschränken sich die Ausführungen des Papiers im Wesentlichen auf die Bundesebene; die Informationsansprüche Betroffener werden nicht erschöpfend dargestellt, der Richtervorbehalt als Instrument des präventiven Rechtsschutzes wird nur gestreift, und das Problem der Verwendung von Geheiminformationen im Strafverfahren wird nicht behandelt.[11]

2 Das Menschenrecht auf wirksame Beschwerde im Staatsschutz

„Jede Person, die in ihren in dieser Konvention anerkannten Rechten oder Freiheiten verletzt worden ist, hat das Recht, bei einer innerstaatlichen Instanz eine wirksame Beschwerde zu erheben, auch wenn die Verletzung von Personen begangen worden ist, die in amtlicher Eigenschaft gehandelt haben", heißt es in Art. 13 der Europäischen Menschenrechtskonvention (EMRK) von 1950. Daran anknüpfend, verpflichten sich die Vertragsstaaten des Internationalen Paktes über bürgerliche und politische Rechte (Zivilpakt) in Art. 2 Abs. 3 „dafür Sorge zu tragen, dass jeder, der in seinen in diesem Pakt anerkannten Rechten oder Freiheiten verletzt worden ist, das Recht hat, eine wirksame Beschwerde einzulegen". Auch wenn der Zivilpakt – anders als die Rechtsweggarantie des Grundgesetzes (Art. 19 Abs. 4 GG) – den gerichtlichen Rechtsschutz mit Rücksicht auf andere Rechtstraditionen nicht ausdrücklich zum Regelfall erklärt, so räumt er diesem durch das Gebot, ihn auszubauen, doch Priorität ein.[12]

Dabei ist zu beachten, so der UN-Menschenrechtsausschuss, dass der Beschwerdeweg zugänglich ist und die Bedürfnisse besonders verletzlicher Gruppen angemessen berücksichtigt. Zudem sind administrative Vorkehrungen zu treffen, damit Beschwerden unverzüglich, gründlich und wirksam durch unabhängige und unparteiische Einrichtungen untersucht werden können.[13] Jedoch können in Fällen, in denen es unmöglich ist, nachträglichen Rechtsschutz zu erwirken, beispielsweise weil Betroffene „verschwunden" sind, auch Maßnahmen zur Prävention solcher Menschenrechtsverletzungen das wirksamere Mittel sein, um einen effektiven Zugang zum Recht zu gewährleisten.[14]

Auch der Europäische Gerichtshof für Menschenrechte (EGMR) und das Bundesverfassungsgericht (BVerfG) haben wiederholt deutlich gemacht, dass dort, wo es unmöglich ist, nachträglichen Rechtsschutz zu erwirken, andere Regeln gelten müssen. So erklärte der EGMR in seinem Grundsatzurteil *Klass und andere gegen Deutschland*, dass Einzelpersonen – anders als den Vertragsstaaten der Europäischen Menschenrechtskonvention – zwar im Prinzip kein Recht zustehe, die abstrakte Prüfung von nationalen Gesetzen zu beantragen, sondern die beschwerdeführende Person unmittelbar durch mutmaßliche Menschenrechtsverletzungen betroffen sein müsse. Allerdings sei ein effektiver Zugang zum Recht verstellt, wenn Menschen aufgrund der Heimlichkeit von Maßnahmen keine Chance hätten, ihre Betroffenheit nachzuweisen und auf dieser Grundlage eine Prüfung der Rechtmäßigkeit zu veranlassen: „Das Gericht akzeptiert daher, dass ein Individuum unter bestimmten Bedingungen behaupten kann, Op-

11 Detaillierte Darstellungen der genannten Bereiche finden sich unter anderem bei Kornblum, Thorsten (2011): Rechtsschutz gegen geheimdienstliche Aktivitäten. Berlin: Dunker & Humblot; Wildhagen, Lars (2011): Persönlichkeitsschutz durch präventive Kontrolle. Richtervorbehalte und nichtrichterliche Kontrollorgane als Ausprägung des Prinzips der Informationsoptimierung bei Grundrechtseingriffen. Berlin: Duncker & Humblot; Rehbein, Mareike (2011): Die Verwertbarkeit von nachrichtendienstlichen Erkenntnissen aus dem In- und Ausland im deutschen Strafprozess. Berlin: Duncker & Humblot.

12 Vgl. Nowak, Manfred (2005): U.N. Covenant on Civil and Political Rights. CCPR. Commentary. 2. Aufl. Kehl u.a.: Engel, S. 58 ff.

13 UN, Human Rights Committee (2004): CCPR General Comment No. 31. The nature of the general legal obligation imposed on states parties to the Covenant. CCPR/C/21/Rev. 1/Add. 13, 29.03.2004, Rn. 15.

14 Vgl. Nowak, Manfred (2005): U.N. Covenant on Civil and Political Rights. CCPR. Commentary. 2. Aufl. Kehl u.a.: Engel, S. 62.

fer einer Rechtsverletzung zu sein, die veranlasst ist durch die bloße Existenz einer geheimen Maßnahme oder Gesetzgebung, die geheime Maßnahmen erlaubt, ohne die tatsächliche Betroffenheit durch solche Maßnahmen nachweisen zu müssen."[15] Im konkreten Fall ging es um die Beschwerde mehrerer bundesdeutscher Rechtsanwälte gegen das Artikel 10-Gesetz, mit dem 1968 nachrichtendienstliche Eingriffe in das Brief-, Post- und Fernmeldegeheimnis autorisiert worden waren. Angesichts der Tatsache, dass damit jede Person in der Bundesrepublik potenziell zum Objekt staatlicher Überwachung werden könnte, ohne den Nachweis unmittelbarer Betroffenheit zu erbringen, erklärte der EGMR die Beschwerde für zulässig: „Die Frage, ob die Beschwerdeführer tatsächlich von einer Verletzung der Konvention betroffen waren, ist verknüpft mit der Feststellung, ob das angegriffene Gesetz selbst mit den Vorschriften der Konvention vereinbar ist."[16]

Ähnlich argumentierte das Bundesverfassungsgericht bereits 1970 in seinem ersten Urteil zum Artikel 10-Gesetz: „Wenn dem Betroffenen die Möglichkeit, sich gegen den Vollzugsakt zu wenden, verwehrt ist, weil er von dem Eingriff in seine Rechte nichts erfährt, muß ihm die Verfassungsbeschwerde unmittelbar gegen das Gesetz ebenso zustehen wie in den Fällen, in denen aus anderen Gründen eine Verfassungsbeschwerde gegen den Vollzugsakt nicht möglich ist."[17] In der Folge erklärte es Beschwerden gegen neue Sicherheitsgesetze immer dann für zulässig, wenn aufgrund der großen Streubreite einer Maßnahme „mit einiger Wahrscheinlichkeit" davon auszugehen sei, dass Personen in ihren Grundrechten beeinträchtigt werden, ohne davon aufgrund einer behördlichen Benachrichtigung Kenntnis zu erlangen: „Die Möglichkeit, eine Verfassungsbeschwerde unmittelbar gegen ein Gesetz zu erheben, das zu heimlichen Maßnahmen berechtigt, entfällt deshalb unter dem Gesichtspunkt der Unmittelbarkeit jedenfalls in der Regel nur, wenn die spätere Kenntniserlangung des Betroffenen durch eine aktive Informationspflicht des Staates rechtlich gesichert ist", bekräftigte das Gericht 2013 in seiner Entscheidung zum Antiterrordateigesetz.[18]

Damit erinnert das Gericht zugleich an die lange Serie von Entscheidungen, mit der es durch die Festschreibung von Verfahrensgarantien Anforderungen für die Verhältnismäßigkeit verdeckter Informationserhebungen definiert: Insbesondere ist – neben dem Gebot, Maßnahmen *vorab* richterlich zu prüfen – *nachträglich* ein individueller Rechtsschutz zu ermöglichen, indem die datenerhebenden Behörden dazu verpflichtet werden, Betroffene nach Beendigung einer Maßnahme zu informieren.[19]

Neben der Notwendigkeit, den individuellen Zugang zum Recht gegenüber heimlichen Maßnahmen durch die nachträgliche Benachrichtigung über eine verdeckte Maßnahme zu sichern, konstatierten jedoch sowohl das Bundesverfassungsgericht als auch der EGMR in seinem Urteil Klass und andere gegen Deutschland die ausnahmsweise Notwendigkeit und Legitimität einer vollständigen Geheimhaltung gegenüber Betroffenen aus Gründen des Staats- und Verfassungsschutzes:

„Zwar verlangt die Rücksicht auf die Subjektqualität des Menschen normalerweise, daß er nicht nur Träger subjektiver Rechte ist, sondern auch zur Verteidigung und Durchsetzung seiner Rechte den Prozeßweg beschreiten und vor Gericht seine Sache vertreten kann, in diesem Sinne also Gerichtsschutz genießt. Es gibt aber seit je Ausnahmen von dieser Regel, die die Menschenwürde nicht kränken. Jedenfalls verletzt es die Menschenwürde nicht, wenn der Ausschluß des Gerichtsschutzes nicht durch eine Mißachtung oder Geringschätzung der menschlichen Person, sondern durch die Notwendigkeit der Geheimhaltung von Maßnahmen zum Schutze der demokratischen Ordnung und des Bestandes des Staates motiviert wird. Dagegen würde die Menschenwürde angetastet, wenn durch den Ausschluß des Rechtswegs der Betroffene der Willkür der Behörden ausgeliefert wäre."[20]

15 „The Court therefore accepts that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him." – EGMR (1978): Klass und andere gegen Deutschland, Urteil vom 06.09.1978, Beschwerde Nr. 5029/71, Rn. 34.

16 „The question whether the applicants were actually the victims of any violation of the Convention involves determining whether the contested legislation is in itself compatible with the Convention's provisions." – Ebda., Rn. 38.

17 BVerfG (1970): Urteil vom 07.07.1970, 2 BvF 1/69. In: BVerfGE 30, 1 (Abhörurteil), S. 1.

18 BVerfG (2013): Urteil vom 24.03.2013, 1 BvR 1215/07, Rn. 84.

19 Siehe u.a. BVerfG (1999): Urteil vom 14.07.1999, 1 BvR 2226/94. In: BVerfGE 100, S. 313 ff. (Telekommunikationsüberwachung I), S. 364; BVerfG (2004): Urteil vom 03.03.2004.,1 BvR 2378/98. In: BVerfGE 109, 279 (Großer Lauschangriff), S. 364 ff.; BVerfG (2005): Urteil vom 27.07.2005., 1 BvR 668/04. In: BVerfGE 113, 348 (Vorbeugende Telekommunikationsüberwachung), S. 389 ff.;

20 BVerfG (1970): Urteil vom 07.07.1970, 2 BvF 1/69. In: BVerfGE 30, 1 (Abhörurteil), S. 27. Es sei daran erinnert, dass die Entscheidung knapp war. Drei von acht Richtern äußerten sich in einem Minderheitsvotum, in dem es unter anderem heißt: „Es sollte nicht mehr besonders betont werden müssen, daß ein Geheimverfahren, wie es in Art. 10 Abs. 2 Satz 2 GG zugelassen ist, also ein Verfahren, in dem der Betrof-

Zu ersetzen, so das Verfassungsgericht weiter, ist der Rechtsweg daher durch eine unabhängige, stetige und effektive Rechtskontrolle, die ausnahmsweise nicht durch Gerichte, sondern auch durch vom Parlament bestellte oder unabhängige Institutionen innerhalb des Funktionsbereichs der Exekutive ausgeübt werden kann.[21] Eben diese außergerichtliche Rechtskontrolle soll für den Arkanbereich der Geheimdienste sicherstellen, dass das Fehlen des individuellen Rechtsschutzes nicht zu Behördenwillkür und Machtmissbrauch einlädt. Primär geht es dabei nicht um die Sicherung parlamentarische Kontrollrechte gegenüber der Exekutive. Vielmehr hat die außergerichtliche Kontrolle eine Wächterfunktion im Sinne der vom Zugang zum Recht ausgeschlossenen Grundrechtsträger. Sind entsprechende Kontrollgremien nicht in der Lage diese Wächterfunktion effektiv wahrzunehmen, so wäre der Ausschluss des Rechtsweges unzulässig. Denn Betroffene wären dann wehrlos der unkontrollierten Macht der Behörden ausgeliefert und damit zum bloßen Objekt exekutiven Handelns degradiert und in ihrer Würde verletzt.

In den Grundsatzurteilen ging es um den konkreten Fall der G 10-Kommission des Deutschen Bundestages, die die Post- und Telekommunikationsüberwachungsanordnungen der Nachrichtendienste des Bundes sowie Begründungen für den Verzicht auf nachträgliche Benachrichtigungen zu prüfen hat und Beschwerden von Menschen nachgehen soll, die glauben, dass sie überwacht werden.

Doch auch dort, wo der individuelle Rechtsschutz nicht völlig ausgeschlossen, aber nur sehr eingeschränkt gewährleistet ist, kommt Kontrollorganen eine entscheidende Rolle zu. So stellte das Bundesverfassungsgericht für den Betrieb der Antiterrordatei fest, dass Auskunftsrechte – als grundlegende Voraussetzung für die Anfechtung einer eventuell rechtswidriger Datenverarbeitung – „nur mit beträchtlichem Verfahrensaufwand realisierbar" seien und der Nutzen von Benachrichtigungspflichten im Vergleich zum damit verbundenen Behördenaufwand zu gering. Daher forderte es regelmäßige und effektive Kontrollen im Zusammenspiel verschiedener Aufsichtsinstanzen, namentlich der Datenschutzbeauftragten von Bund und Ländern und der G 10-Kommission.[22]

Zusammengefasst ist festzuhalten, dass für den Zugang zum Recht im Bereich der Terrorismus- und Extremismusbekämpfung besondere Regeln gelten: Zum einen ist der Sonderfall abstrakter Normenprüfung – beim Bundesverfassungsgericht „Rechtssatzverfassungsbeschwerde" genannt – eröffnet, da eine unmittelbare Betroffenheit durch heimliche Maßnahmen in der Regel nicht nachweisbar ist. Dann allerdings gilt in Deutschland nach Inkrafttreten des angegriffenen Gesetzes eine Jahresfrist,[23] und beim EGMR muss der nationale Rechtsweg zuerst ausgeschöpft sein – in jedem Fall spielt Zeit eine entscheidende Rolle. Zum anderen aber ist das Menschenrecht auf wirksame Beschwerde dahingehend zu interpretieren, dass es dort, wo der individuelle Nachweis einer Rechtsverletzung aufgrund von Geheimhaltung unmöglich oder wesentlich erschwert ist, besondere Kontrollorgane braucht, deren Aufgabe darin besteht, Machtmissbrauch und behördliche Willkür zu beschränken und verhindern. Dass das Recht auf wirksame Beschwerde auch nach dem 11. September 2001 unvermindert Gültigkeit hat, haben auch internationale Menschenrechtsgremien immer wieder betont.[24]

Wie also steht es um die Nachweisbarkeit der Betroffenheit in Deutschland und wie um das Kontrollgerüst

fene nicht gehört wird und sich nicht verteidigen kann, keinen Rechtsschutz bietet. […] Es bedarf keiner weiteren Erläuterung, daß der Schritt vom verfassungsfremden Zustand der Postkontrolle durch Dienststellen fremder Mächte zu einer verfassungswidrigen Regelung, keinen Schritt näher an das Grundgesetz heranführt' und daß Art. 10 Abs. 2 Satz 2 GG kein Provisorium ist." (S. 43 f.).

21 Ebda., S. 30.

22 BVerfG (2013): Urteil vom 24.03.2013, 1 BvR 1215/07, Rn. 208 ff.

23 § 93 Abs. 3 Bundesverfassungsgerichtsgesetz (BVerfGG).

24 CoE, Venice Commission (2007): Report on the democratic oversight of the security services. Adopted by the Venice Commission at its 71st Plenary Session (Venice, 1–2 June 2007). CDL-AD(2007)016, Strasbourg (Study 388/2006), 11.06.2007, Rn. 122 ff.; UN, Human Rights Council (2009): Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin. UN-Doc. A/HRC/10/3, 04.02.2009. Rn. 58–63; UN, General Assembly (2014): Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. UN-Doc. A/69/397, 23.09.2014, Rn. 48 f.; UN, Human Rights Council (2014): The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. UN-Doc. A/HRC/27/37, 30.06.2014, Rn. 39–41; CoE, Commissioner for Human Rights (2015): Positions on counter-terrorism and human rights protection. CommDH/PositionPaper(2015)1. Council of Europe: Strasbourg; CoE, Venice Commission (2015): Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies. Adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20–21 March 2015) on the basis of comments by Mr Iain Cameron (Member, Sweden). CDL-AD(2015)006. Strasbourg (Study 719/2013), 07.04.2015, Rn. 137 f.; CoE, Commissioner for Human Rights (2015): Democratic and effective oversight of national security services. Council of Europe: Strasbourg (Issue Paper), S. 26 f.

für die neue „Sicherheitsarchitektur"? Welche Möglichkeit haben Menschen, die als Terror- oder Extremismusverdächtige in den Fokus von Sicherheitsbehörden geraten sind, die Gerichte anzurufen, um den gegen sie gerichteten Verdacht überprüfen zu lassen und gegebenfalls daraus erwachsene Nachteile zu kompensieren? Und welche Mittel haben Aufsichtsinstanzen, um stellvertretend für Betroffene Licht in die dunklen Ecken des Rechtsstaates zu bringen und gegebenenfalls Recht wieder herzustellen?

3 Rechtsschutz im Staatsschutz?

3.1 Verdeckte Maßnahmen und Benachrichtigungspflichten

Gilt für Datenerhebungen, die für Betroffene nicht ersichtlich sind nach § 4 Abs. 3 Bundesdatenschutzgesetz (BDSG) grundsätzlich eine unmittelbare Unterrichtungspflicht, so ist diese für Sicherheitsbehörden durch Spezialklauseln suspendiert (beispielsweise § 37 BKAG, § 37 BPolG, § 27 BVerfSchG). Stattdessen gelten für polizeiliche Maßnahmen zur verdeckten Informationsbeschaffung in der Regel nachträgliche Benachrichtigungspflichten,[25] so dass Betroffene theoretisch nach Ende der Maßnahme die Möglichkeit haben, deren Rechtmäßigkeit gerichtlich prüfen zu lassen. Erstmals geregelt wurden solche Benachrichtigungspflichten mit Inkrafttreten des Artikel-10-Gesetzes im Jahr 1968. Geändert wurde damals § 101 Abs. 1 der Strafprozessordnung: „Von den getroffenen Maßregeln (§§ 99, 100, 100a, 100b) [Postbeschlagnahme und Überwachung des Fernmeldeverkehrs] sind die Betroffenen zu benachrichtigen, sobald dies ohne Gefährdung des Untersuchungszwecks geschehen kann." Seitdem wurde die Liste der verdeckten Maßnahmen sukzessive erweitert – unter anderem um Rasterfahndungen, „große Lauschangriffe", längerfristige Observationen oder den Einsatz von Mobilfunkmasten simulierenden IMSI-Catchern und Verdeckten Ermittlern – und auch die Vorgaben zur Benachrichtigungspflicht wurden erheblich modifiziert. Inzwischen sind Betroffene mit der Benachrichtigung ausdrücklich auf die Möglichkeit nachträglichen Rechtsschutzes hinzuweisen. Wollen sie davon Gebrauch machen, bleiben ihnen nur zwei Wochen Zeit, die Prüfung der Rechtmäßigkeit zu beantragen.[26] Allerdings kann mit Zustimmung eines Gerichts von einer Benachrichtigung abgesehen werden, wenn Gefährdungen des Untersuchungszwecks oder für Leib, Leben oder Freiheit einer Person und von bedeutenden Vermögenswerten „mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft vorliegen werden".[27] Unter besonderen Umständen wird also die Möglichkeit nachträglichen Rechtsschutzes vollständig durch eine richterliche Kontrolle ersetzt.

Ähnliche Vorschriften zur Benachrichtigung finden sich auch im Polizeirecht von Bund und Ländern für verdeckte Präventivmaßnahmen. Allerdings ist dort nicht in jedem Fall das Unterlassen der Benachrichtigung richterlich zu prüfen, sondern teilweise nur die Gründe aktenkundig zu machen.[28] Auch bleibt mitunter offen, wie lange das Zurückstellen von Benachrichtigungen möglich ist, so dass keine Verfahrenssicherheit gewährleistet ist.[29] Zudem finden sich Regelungen nach denen eine Benachrichtigung unterbleiben kann, wenn eine Gefährdung der „öffentlichen Sicherheit" befürchtet wird, obwohl das Bundesverfassungsgericht in seinem Urteil zum „Großen Lauschangriff" gerügt hatte, dass mit dem Begriff der „öffentlichen Sicherheit" die Suspendierung der Benachrichtigungspflicht unter eine Generalklausel gestellt sei.[30] Entsprechend unterliegt die Ausgestaltung der Benachrichtigungspflichten im polizeirechtlichen Bereich im Detail erheblichen verfassungsrechtlichen Bedenken.

Ein zusätzliches Problem stellt sich durch die beschleunigte technische Innovation, die ihrer Verrechtlichung heute immer einen Schritt voraus ist. Zwar verlangt das Bestimmtheitsgebot, so das Bundesverfassungsgericht in seinem Urteil zur GPS-Observation, dass der Gesetzgeber den für den Grundrechtsschutz riskanten informationstechnischen Wandel aufmerk-

25 Im Nachrichtendienstrecht ist für die Pflicht zur Benachrichtigung von Betroffenen nach Beendigung einer verdeckten Maßnahme der Begriff „Mitteilungspflicht" üblich. Der Verständlichkeit halber wird hier jedoch durchgängig von „Benachrichtigungspflichten" gesprochen.

26 Kritisch zur kurzen Frist und mit der Auffassung, dass bei richterlich angeordneten Maßnahmen Rechtsschutz auch parallel auf dem Weg der Beschwerde nach §§ 304 ff. StPO erlangt werden kann Singelnstein, Tobias (2009): Rechtsschutz gegen heimliche Ermittlungsmaßnahmen nach Einführung des § 101 VII 2–4 StPO. In: Neue Zeitschrift für Strafrecht (9/2009), S. 481–486.

27 § 101 Abs. 6 StPO.

28 Z. B. § 22a Abs. 4 BPolG und § 7 Abs. 6 BKAG.

29 Z. B. § 28 Abs. 5 BPolG.

30 Vgl. Schenke, Wolf-Rüdiger (2014): Bundespolizeigesetz § 28. In: Schenke, Wolf-Rüdiger / Graulich, Kurt / Ruthig, Josef (Hg.): Sicherheitsrecht des Bundes. München: C. H. Beck, S. 207; BVerfG (1999): Urteil vom 03.03.2004, 1 BvR 2378/98. In: BVerfGE 109, 279 (Großer Lauschangriff), S. 366. Siehe zur Kritik an den bestehenden Benachrichtigungspflichten auch Bäcker, Matthias / Giesler, Volkmar / Harms, Monika / Hirsch, Burkhard / Kaller, Stefan / Wolff, Heinrich Amadeus (2013): Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland. Berlin: BMI und BMJ, S. 239 ff.

sam beobachtet, um korrigierend einzugreifen und technische Eingriffsinstrumente genau zu bezeichnen. „Das Bestimmtheitsgebot verlangt aber keine gesetzlichen Formulierungen, die jede Einbeziehung kriminaltechnischer Neuerungen ausschließe."[31] Somit können verdeckte Überwachungsmaßnahmen mit neuen technischen Mitteln solange unreguliert und damit auch ohne ausdrückliche Pflicht zur Benachrichtigung der Betroffenen stattfinden, bis der Gesetzgeber nachsteuert und Instrumente, die bis dato in einer rechtlichen Grauzone zum Einsatz kamen, explizit verrechtlicht. Ein Beispiel aus der jüngeren Vergangenheit ist das Versenden sogenanner „stiller SMS" zur Erstellung von Bewegungsprofilen.

Jenseits der rechtlichen Grenzen von Benachrichtigungspflichten, haben sich in der Vergangenheit allerdings auch erhebliche praktische Defizite gezeigt, durch die Betroffene ihres Zugangs zum Recht beraubt wurden. Im Jahr 2003 kam ein Gutachten des Max-Planck-Institutes für ausländisches und internationales Strafrecht bei der Auswertung von mehr als 600 Strafverfahrensakten aus den späten 1990er Jahren zu dem ernüchternden Ergebnis, dass es bei zwei Dritteln aller 2.370 Fälle von angeordneten Telekommunikationsüberwachungen (TKÜ), die sich in den Akten fanden, keinen Hinweis darauf gab, dass die gebotene Benachrichtigung der Betroffenen stattgefunden habe. Die Gründe scheinen vielfältig und reichen von ermittlungstaktischen Erwägungen, über die Annahme, dass Betroffene durch Folgemaßnahme ohnehin über die Überwachung informiert würden bis hin zur Wahrnehmung der Benachrichtigungspflicht als „lästige Pflicht".[32] Zwar wurde die Regelung zur Benachrichtigungspflicht seitdem durch das Gesetz zur Neuordnung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen im Jahr 2007 überarbeitet.[33] Ob sich die Lücke zwischen Rechtsanspruch und Rechtswirklichkeit im Gefolge der Neuordnung geschlossen hat ist nicht bekannt. Praktiker stellen jedoch fest, dass die „Neuregelung der Benachrichtigung […] einen nicht unerheblichen administrativen Mehraufwand für die Ermittlungsbehörden mit sich" bringe.[34] Dass sich daraus auch tatsächliche Vollzugsdefizite ergeben, zeigte sich bei der Überprüfung der Funkzellenabfragepraxis in Berlin, bei der der Berliner Datenschutzbeauftragte 2012 feststellte, dass Betroffene „in der Regel nicht bzw. im Hinblick auf die ihnen zustehenden Rechtsschutzmöglichkeiten nur unzureichend benachrichtigt" werden.[35] Da die Ermittlungsverfahren häufig mangels hinreichenden Tatverdachts eingestellt wurden, entfiel auch das Bekanntwerden der Überwachung im Rahmen einer Gerichtsverhandlung.

Sind die Möglichkeiten des individuellen Rechtsschutzes aufgrund nachträglicher behördlicher Benachrichtigungspflichten im Bereich von Polizei und Strafverfolgung somit rechtlich wie praktisch begrenzt, so sind die Hürden für den Zugang zum Recht im Feld der nachrichtendienstlichen Überwachung mit wenigen Ausnahmen noch einmal deutlich höher. „Das Bundesamt für Verfassungsschutz darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung, wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen anwenden. Diese sind in einer Dienstvorschrift zu benennen, die auch die Zuständigkeit für die Anordnung solcher Informationsbeschaffungen regelt. Die Dienstvorschrift bedarf der Zustimmung des Bundesministeriums des Innern, der das Parlamentarische Kontrollgremium unterrichtet", heißt es beispielsweise in § 8 Abs. 2 BVerfSchG.

Eine Benachrichtigungspflicht besteht dabei allerdings nur in Fällen eines „großen Lauschangriffs", also dem Abhören von Wohnräumen, oder bei Maßnahmen der heimlichen Informationsbeschaffung, „die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen" – genannt wird insbesondere das Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem verdeckten Einsatz technischer Mittel. In all diesen Fällen

31 BVerfG (2005): Urteil vom 12.04.2005, Aktenzeichen 2 BvR 581/01, Rn. 51.

32 Albrecht, Hans-Jörg u.a. (2003): Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen. Abschlussbericht. Max-Planck-Institut für ausländisches Strafrecht und Kriminologie, Freiburg. (Kriminologische Forschungsberichte). http://www.mpicc.de/ww/de/pub/forschung/forschungsarbeit/kriminologie/archiv/tkue.htm (Stand: 12.08.2014), S. 276 ff. Zur sehr ähnlichen Ergebnissen kamen Backes, Otto / Gusy, Christoph (2003): Wer kontrolliert die Telefonüberwachung? Frankfurt am Main: Peter Lang.

33 Deutscher Bundestag (2007): Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG. Gesetzentwurf der Bundesregierung. Drucksache 16/5846, 27.06.2007.

34 Bohnen, Wolfgang (2009): Benachrichtigungen über Telekommunikationsüberwachungsmaßnahmen nach dem Gesetz zur Neuregelung der Telekommunikationsüberwachung. In: Die Kriminalpolizei (2/2009), S. 26–29 (29).

35 Berliner Beauftragter für Datenschutz und Informationsfreiheit (2012): Abschlussbericht zur rechtlichen Überprüfung von Funkzellenabfragen. Berlin. http://datenschutz-berlin.de/attachments/896/Pr__fbericht.pdf (PDF, 148 KB, Stand: 09.08.2015), S. 17.

sind Betroffene nach Beendigung der Maßnahme zu benachrichtigen, „sobald eine Gefährdung des Zweckes des Eingriffs ausgeschlossen werden kann".[36] Anders als im Bereich von Strafverfolgung und Polizei ist allerdings nicht vorgesehen, dass das Vorliegen beziehungsweise Nichtvorliegen dieser Voraussetzung gerichtlich überprüft wird. Nur das Parlamentarische Kontrollgremium ist in diesen Fällen über Einzelmaßnahmen zu informieren und könnte gegebenenfalls prüfen, ob eine individuelle Benachrichtigung widerrechtlich ausgeblieben ist. Jenseits dessen, zum Beispiel bei längeren Observationen und dem Einsatz von V-Leuten oder IMSI-Catchern, so die herrschende Meinung, besteht keine Benachrichtigungspflicht.[37]

Nachträglich zu benachrichtigen sind Betroffene auch bei einer individuellen Brief-, Post- und Fernmeldeüberwachung nach Artikel 10-Gesetz und seit 2002 auch, wenn die Nachrichtendienste bei Fluggesellschaften, Geldinstituten, Telekommunikations- und Telemediendienstleistern „besondere Auskünfte" verlangen. Die Benachrichtigung unterbleibt, „solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist".[38] Wenn Betroffene auch ein Jahr nach Beendigung der Maßnahme immer noch nicht benachrichtigt wurden, bedarf eine weitere Zurückstellung der ausdrücklichen Zustimmung durch die G 10-Kommission. Ist die G 10-Kommission nach fünf Jahren einstimmig der Meinung, dass die Voraussetzung für den Verzicht auf Benachrichtigung „mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft" vorliegen werden, kann auf die Mitteilung gänzlich verzichtet werden.

3.2 Intransparente Datenverarbeitung und das Recht auf Auskunft

Äußerst schwierig kann es auch sein, wenn Betroffene aktiv werden (müssen), um Kenntnis darüber zu erlangen, ob und wenn ja, warum sie in Systemen der polizeilichen oder nachrichtendienstlichen Datenverarbeitung erfasst sind. Das zentrale Instrument hierfür ist das Auskunftsrecht, das Betroffene erst in die Lage versetzt, weitere Rechte wie die Korrektur falscher oder die Löschung rechtswidrig gespeicherter Daten zu erzwingen oder Schadensersatzforderungen geltend zu machen. Als „Magna Charta" des Datenschutzrechts ist es grundlegende Voraussetzung für einen effektiven Rechtsschutz, der voraussetzt, dass Menschen sich Kenntnis über die Verarbeitung sie betreffenden Daten verschaffen können.[39]

Waren Sicherheitsbehörden lange Zeit überhaupt nicht zur Auskunft verpflichtet, so wurden auf Bundesebene mit dem Gesetz über die Fortentwicklung der Datenverarbeitung und des Datenschutzes von 1990 Ansprüche von Betroffenen gegenüber Polizei, Strafverfolgungsbehörden und Nachrichtendiensten rechtlich verankert. Jedoch gilt das Auskunftsrecht nicht in jedem Fall.

So hat die Auskunft durch Polizeibehörden des Bundes oder die Staatsanwaltschaft gemäß § 19 BDSG beziehungsweise § 491 StPO etwa zu unterbleiben, wenn dadurch die ordnungsgemäße Aufgabenerfüllung einer verantwortlichen Stelle oder die öffentliche Sicherheit oder Ordnung gefährdet wäre, beispielsweise weil laufende Ermittlungen bekannt würden, Nachteile für das Wohl des Bundes oder eines Landes drohten oder Interessen Dritter überwögen. Eine Ablehnung bedarf keiner Begründung, wenn der mit einer Auskunftsverweigerung verfolgte Zweck dadurch gefährdet wäre. In einem solchen Fall können Betroffene allerdings die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) einschalten, damit ihre Behörde stellvertretend prüft, ob ein rechtswidriger Eingriff in das Persönlichkeitsrecht vorliegt. Die verantwortliche Stelle hat der BfDI in vollem Umfang Auskunft zu erteilen; allerdings darf die anschließende Mitteilung an die betroffene Person keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, um eine Ausforschung durch Einschaltung der Bundesdatenschutzbeauftragten zu verhindern. Eine Ausnahme von diesem „Ersatzrecht" gibt es jedoch: Wenn das jeweils zuständige Bundesministerium gemäß § 24 Abs. 4 BDSG im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde, kann es die Auskunft selbst gegenüber sicherheitsüberprüften BfDI-Mitarbeitenden verweigern.[40]

36 § 9 Abs. 3 BVerfSchG.
37 Mallmann, Otto (2014): Bundesverfassungsschutzgesetz § 9. In: Schenke, Wolf-Rüdiger / Graulich, Kurt / Ruthig, Josef (Hg): Sicherheitsrecht des Bundes. München: C.H. Beck, S. 1201 f.
38 § 12 G 10.
39 Mallmann, Otto (2011): § 19 Auskunft an die Betroffenen. In: Simitis, Spiros (Hg.): Bundesdatenschutzgesetz. Kommentar, Baden-Baden: Nomos, 7. Auflage, S. 984.
40 Mit § 15 Abs. 4 BVerfSchG findet sich eine solche Regelung auch im Recht der Dienste.

Gilt diese Sonderregel, nach der Betroffene ihr Auskunftsrecht weder direkt noch indirekt wahrnehmen können, als „Notstandsklausel", deren Anwendung nur in extremen Ausnahmefällen in Betracht käme,[41] so sind Auskunftssuchende gegenüber den Nachrichtendiensten zudem häufig mit Spezialklauseln konfrontiert, die zum einen hohe Voraussetzungen für einen Auskunftsanspruch anlegen und ihm zum anderen enge Grenzen setzen. So müssen Betroffene gegenüber den Diensten des Bundes und der meisten Länder auf einen „konkreten Sachverhalt" hinweisen und ein „besonderes Interesse" an der Auskunft darlegen.[42] Das heißt: Auskunftssuchende müssen einem Nachrichtendienst erstens zunächst Informationen über sich liefern, worin viele die Gefahr sehen, sich selbst verdächtig zu machen und erfasst zu werden, auch wenn ursprünglich keine Informationen zur Person gesammelt worden waren. Zweitens muss das Interesse des Auskunftssuchenden das generelle Geheimhaltungsinteresse des Dienstes überwiegen, beispielsweise weil die Kenntnis der Informationen zur Geltendmachung individueller Rechte in einem Verwaltungs- oder Gerichtsverfahren erforderlich ist. Doch selbst wenn diese Hürden genommen sind, kann die Auskunftserteilung verweigert werden, wenn die Gefährdung der Aufgabenerfüllung, des Quellenschutz oder allgemein der öffentlichen Sicherheit befürchtet wird. Obwohl Auskunftssuchende grundsätzlich Anspruch auf die Begründung einer Ablehnung haben, kann der Dienst darauf verzichten, soweit der Zweck der Auskunftsverweigerung dadurch gefährdet wäre. Im Ergebnis werden auf dieser Grundlage Auskünfte fast nie erteilt: „Zwar hat der Bürger einen grundsätzlichen Auskunftsanspruch; ob die Behörde diesen Anspruch allerdings erfüllt hat, kann er regelmäßig nicht überprüfen. […] Praktische Folge des fehlenden Auskunftsanspruchs und des weiten Ermessens der Verfassungsschutzämter ist: Im Regelfall wird von der Auskunft abgesehen."[43] Dann bleibt nur der Gang vors Verwaltungsgericht. Dieser jedoch ist, wie weiter unten im Kapitel zu „Geheiminformationen vor Gericht" gezeigt wird, steinig und langwierig.

Dabei ist die Auskunft über die gespeicherten Daten nur der erste Schritt, um die Rechtmäßigkeit ihrer Erhebung, Speicherung und Weiterverarbeitung prüfen zu lassen und gegebenenfalls eine Löschung oder Korrektur zu erwirken. Dass solche Überprüfungen gerade im relativ abgeschotteten Bereich von Staats- und Verfassungsschutz ihre Notwendigkeit und Berechtigung haben, zeigen zwei Beispiele aus den letzten Jahren: So veranlasste die Eingabe eines Betroffenen den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im März 2012 zur Prüfung der BKA-Zentraldatei „Politisch-motivierte Kriminalität links". Bei der Prüfung wurden strukturelle Defizite insbesondere bei der Erfassung „sonstiger Personen"[44] deutlich, die nicht nur die eine Datei, sondern die gesamte Dateienlandschaft des Staatsschutzes beim Bundeskriminalamt (BKA) betrafen. Im Ergebnis kam es zu umfangreichen Löschungen von Daten sowie einer Fortbildung der Sachbearbeiter mit dem Ziel der Sensibilisierung für die Rechtslage.[45]

Beim Verfassungsschutz Niedersachsen kam es nach dem nur zufällig ans Licht gekommenen Skandal um die widerrechtliche Registrierung von Journalistinnen und Journalisten zur Überprüfung der Amtsdatei durch eine „Task Force" externer Fachleute, die zu dem Ergebnis kamen, dass etwa ein Fünftel aller in der Datei erfassten Personen rechtswidrig gespeichert waren. Da außerdem die Speicherung zahlreicher weiterer Daten nicht länger zur Aufgabenerfüllung erforderlich war, wurden im Ergebnis 40 Prozent der rund 9.000 Personendatensätze gelöscht.[46]

3.3 Schutzlücken in der internationalen Zusammenarbeit

An Grenzen stoßen Auskunftsansprüche auch im Kontext der wachsenden internationalen Zusammenarbeit von Sicherheitsbehörden. So garantiert Art. 58 des EU-Ratsbeschlusses über das Schengen-Informationssystem der zweiten Generation (SIS II) – einem europaweiten polizeilichen Fahndungssystem, in dem mehr als 700.000 Personen erfasst sind – jeder Person ein Recht auf Auskunft zu über sie gespeicherten Daten zu. Allerdings richtet sich der Auskunftsanspruch nach

41 Ebda., S. 1008.

42 So die Regelung bei Anfragen beim Bundesamt für Verfassungsschutz laut § 15 Abs. 1 BVerfSchG. Einige Landesnormen, z. B. in Brandenburg oder Berlin, legen die Hürden weniger hoch.

43 Gusy, Christoph (2011): Grundrechte und Verfassungsschutz, 1. Aufl., Wiesbaden: VS Verlag, S. 103.

44 Gemeint sind Personen, deren Daten nach § 8 Abs. 5 BKAG verarbeitet werden dürfen, „weil bestimmte Tatsachen, die Annahme rechtfertigen, daß die Betroffenen Straftaten von erheblicher Bedeutung begehen werden".

45 Vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2013): 24. Tätigkeitsbericht 2011-2012. Bonn, S. 96 f.; Deutscher Bundestag (2015): Staatsschutzdateien von Sicherheitsbehörden des Bundes. Drucksache 18/5659, 29.07.2015.

46 Niedersächsisches Ministerium für Inneres und Sport (Hg.) (2014): Abschlussbericht der Task Force zur Überprüfung der Speicherung personenbezogener Daten durch den Niedersächsischen Verfassungsschutz. Hannover. http://www.mi.niedersachsen.de/download/87237 (PDF, 259 KB, nicht barrierefrei, Stand: 21.08.2015).

dem nationalen Recht des jeweiligen EU-Mitgliedstaates, in dessen Hoheitsgebiet das Auskunftsrecht geltend gemacht wird. Zudem hat ein Mitgliedstaat, auf dessen Territorium um Auskunft ersucht wird, zuerst den ausschreibenden Mitgliedstaat zu konsultieren. Eine Auskunftserteilung kann dann unterbleiben, wenn „dies zur Durchführung einer rechtmäßigen Aufgabe im Zusammenhang mit einer Ausschreibung [...] unerlässlich ist."[47] Insbesondere im Fall von laufenden Ausschreibungen zur verdeckten oder gezielten Kontrolle nach Art. 36 SIS II-Beschluss wird die Auskunft regelmäßig verweigert.[48] Solche Ausschreibungen dienen der Überwachung von Zielpersonen, mittels derer Reisewege, aber auch Begleitpersonen und mitgeführte Sachen ausgeforscht werden sollen. Betroffen von einer solchen Ausschreibung waren im Jahr 2014 mehr als 46.000 Menschen.[49] Wenn das nationale Recht es erlaubt, können auf diesem Wege auch Staatsschutzstellen und Nachrichtendienste, wie der deutsche Verfassungsschutz,[50] die Ausschreibung von Personen veranlassen, wenn sie Anhaltspunkte haben, dass von diesen erhebliche Gefahren für die innere oder äußere Sicherheit ausgehen. Das BKA beziehungsweise Verfassungsschutz, Bundesnachrichtendienst (BND) oder Militärischer Abschirmdienst (MAD) sind zwar dazu verpflichtet, Betroffene nach Beendigung einer solchen Ausschreibung zu benachrichtigen – dies allerdings nur, wenn Ausschreibungen durch deutsche Stellen vorgenommen wurden und Aufgaben im Zusammenhang mit der Ausschreibung nicht gefährdet würden.[51] Im Fall einer Ausschreibung durch ausländische Stellen ist das BKA verpflichtet, verweigerte Auskünfte nach Beendigung der Maßnahme zu erteilen. Hierzu muss jedoch eine positive Stellungnahme der ausschreibenden Stelle vorliegen.[52] Das bedeutet: Wenn die schwedische Sicherheitspolizei oder der französische Staatsschutz Menschen europaweit zur verdeckten Kontrolle ausschreibt und damit auch Maßnahmen deutscher Behörden veranlasst, ist der Zugang der Betroffenen zum Recht in Deutschland davon abhängig, dass das schwedische oder französische Recht vergleichbare Pflichten zur nachträglichen Auskunftserteilung oder Benachrichtigung kennen wie das BKA-Gesetz.

Sind im Bereich der europäischen Polizei- und Justizkooperation Auskunftsrechte Betroffener innerhalb der aufgezeigten Grenzen noch verbrieft, kennt das Feld der interkontinentalen Zusammenarbeit ein solches Recht teilweise gar nicht. So heißt es etwa im bilateralen deutsch-amerikanischen „Preventing and Combating Serious Crime"-Abkommen von 2008 ausdrücklich: „Aus diesem Abkommen erwachsen Privatpersonen keine Rechte".[53] Obwohl die Vertragsparteien sich auch zur spontanen Übermittlung von „relevanten" Personendaten zur Verhinderung terroristischer Straftaten verpflichten,[54] gelten für den Umgang mit den übermittelten Daten und eventueller Bedingungen für die Weiterverwendung „Treu und Glauben" und die jeweiligen nationale Rechtsvorschriften.[55] Auskunftsrechte existieren in den Vereinigten Staaten für Nicht-US-Bürger allerdings nicht. Stattdessen ermächtigt das deutsche Umsetzungsgesetz Betroffene, Auskunftsersuchen an das BKA als nationale Kontaktstelle für den transatlantischen Informationsaustausch zu richten, die von dort an die zuständigen US-amerikanischen Behörden zur Beantwortung weitergeleitet werden. Die Auskunftserteilung darf von den US-Behörden allerdings aufgrund nationaler Rechtsvorschriften verweigert werden, einschließlich in Fällen, in denen die wie auch immer gearteten „Zwecke der Verarbeitung" gefährdet wären – diese Zwecke können, die Zustimmung der deutschen Vertragspartei vorausgesetzt, alles Mögliche sein.[56] Zudem kann das BKA unter gleichlautenden Bedingungen wie nach § 19 Abs. 4 Bundesdatenschutzgesetz davon absehen, Betroffene über die von US-Stellen erhaltenen Informationen zu unterrichten.[57] Zahlreich sind somit die Möglichkeiten, eine Auskunft zu verweigern. Vor diesem Hintergrund

47 Art. 58 Beschluss 2007/533/JI des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengen-Informationssystems der zweiten Generation (SIS II-Beschluss).

48 Im alten Schengener Durchführungsübereinkommen war dies in Art. 102 Abs. 2 Satz 2 noch explizit so geregelt: „Sie [die Auskunftserteilung] unterbleibt immer während der Ausschreibung zur verdeckten Registrierung.

49 eu-LISA (2015): SIS II – 2014 statistics, EU-Ratsdok. 7925/15 vom 15.04.2015, S. 12.

50 § 17 Abs. 3 BVerfSchG.

51 § 15a Abs. 1 und 2 Bundeskriminalamtgesetz (BKAG).

52 § 15a Abs. 3 BKAG i.V.m. Art. 58 Abs. 3 SIS II-Beschluss.

53 Art. 11 Abs. 3 Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität v. 01.10.2008 (PCSC-Abkommen).

54 Art. 10 PCSC-Abkommen.

55 Art. 11 Abs. 2 PCSC-Abkommen.

56 Art. 17 Abs. 2 PCSC-Abkommen. Zur uferlosen Zweckbestimmung s. Art. 13 Abs. 1d des Abkommens.

57 § 5 Gesetz zur Umsetzung des Abkommens zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika vom 1. Oktober 2008 über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität v. 11.09.2008.

und angesichts der massiven Bedeutung, die die Analyse großer Datenbestände und der behördenübergreifende Informationsaustausch seit dem 11. September 2001 in den USA erhalten haben, scheinen die Aussichten darauf, falsche oder rechtswidrig an die USA übermittelte Daten jemals wieder korrigieren oder löschen zu lassen, denkbar gering.[58]

3.4 Geheiminformationen vor Gericht

Geht es beim Rechtsschutz durch Benachrichtigungspflichten und Auskunftsrechte darum, heimliche Maßnahmen sichtbar zu machen, um sie notfalls gerichtlich zu hinterfragen, so ist der Zugang zum Recht auch dann herausgefordert, wenn offensichtliche Maßnahmen auf geheimen Informationen beruhen. Besonders deutlich zeigt sich das Problem bei den sogenannten „Terrorlisten", auf denen – häufig aufgrund von nachrichtendienstlichen Informationen – als terrorismusverdächtig eingestufte Einzelpersonen und Organisationen gelistet und mit „gezielten Sanktionen", etwa dem Einfrieren von Vermögen und Konten oder Reisebeschränkungen, belegt werden, ohne dass es ein öffentliches Strafverfahren und Gerichtsurteil gegeben hat. Obwohl die Sanktionierung aufgrund der drastischen nicht nur wirtschaftlichen Konsequenzen als „zivile Todesstrafe" bezeichnet wurde,[59] wurde den Betroffenen anfangs eine detaillierte Begründung vorenthalten, die effektiv anfechtbar gewesen wäre. Trotz deutlicher menschenrechtlicher Kritik an dem kafkaesken Verfahren, das durch die Resolution 1267 des UN-Sicherheitsrates im Jahr 1999 installiert worden war, blieben Reformen halbherzig: Zwar können Betroffene gegen Entscheidungen des sogenannten „Taliban-Sanktionskomitees" seit 2010 eine Ombudsperson anrufen, rückgängig machen kann diese die Entscheidungen allerdings nicht, sondern nur Empfehlungen aussprechen.

Erfolgreicher waren Klagen gegen die beiden Terrorlisten der Europäischen Union, mit denen zum einen Resolution 1267 umgesetzt und die Liste des Taliban-Sanktionskomitees kopiert und zum anderen eine autonome Liste aufgrund der Sicherheitsrats-Resolution 1373 vom September 2001 geführt wird. Bereits 2007 reagierte die Union auf das Urteil des Europäischen Gerichtshofes (EuGH) zur Listung der iranischen Volksmudschaheddin vom Vorjahr und entschied, dass Betroffenen eine hinreichend detaillierte Begründung ihrer Sanktionierung aufgrund von Resolution 1373 mitzuteilen sei, damit nicht zuletzt die europäischen Gerichte in die Lage versetzt werden, Entscheidungen zu überprüfen. Im Fall Kadi entschied der EuGH 2008 schließlich sogar gegen die automatische und unhinterfragte Übernahme der Entscheidungen des Taliban-Sanktionskomitees mit der Begründung, dass die Union auch bei der Umsetzung völkerrechtlicher Verpflichtungen – in diesem Fall jene aus Resolution 1267 – an die EU-Grundrechtecharta gebunden sei und entsprechend gerichtlichen Rechtsschutz zu gewährleisten habe. Da dies nicht gegeben war, annullierte das Gericht im Fall Kadi die Verordnung zur Umsetzung des UN-Sanktionsregimes.[60] In seiner zweiten Entscheidung zum Fall Kadi machte der Gerichtshof 2013 dann deutlich, dass es im Bereich der Terrorismusbekämpfung durchaus Informationen geben könne, die aus Sicherheitsgründen gegenüber Betroffenen geheim gehalten werden müssten. Dies dürfe aber nicht dazu führen, dass der individuelle Rechtsschutz ausgehebelt werde, weil auch die Gerichte keinen Zugang zu Beweismaterial erhielten. Obwohl nicht in der Verfahrensordnung des Gerichtshofes vorgesehen, installierte er mit dem Kadi II-Urteil die Möglichkeit eines „in camera"-Verfahrens, d. h. eines Verfahrens, bei dem das Gericht Einsicht in geheime Unterlagen nehmen kann, ohne dass diese Betroffenen über Akteneinsichtsrechte zugänglich werden:

„Zwar können zwingende Erwägungen der Sicherheit oder der Gestaltung der internationalen Beziehungen der Union oder ihrer Mitgliedstaaten der Mitteilung bestimmter Informationen oder Beweise an die betroffene Person entgegenstehen. In einem solchen Fall muss allerdings der Unionsrichter, dem die Geheimhaltungsbedürftigkeit oder Vertraulichkeit dieser Informationen oder Beweise nicht entgegengehalten werden kann, im Rahmen der von ihm ausgeübten gerichtlichen Kontrolle Techniken anwenden, die es ermöglichen, die legitimen Sicherheitsinteressen in Bezug auf die Art und die Quellen der Informationen, die beim Erlass des betreffenden Rechtsakts berücksichtigt wurden, auf der einen Seite und das Erfordernis, dem Einzelnen die Wahrung seiner Ver-

58 Hieran dürfte sich auch durch die Mitte September 2015 angekündigte Unterzeichnung des Datenschutzabkommens zwischen der EU und den USA nichts ändern, da dieses existierende nationale Abkommen nur ergänzen, aber nicht ersetzen soll. Vgl. European Commission (2015): Questions and Answers on the EU-US data protection „Umbrella agreement". Fact Sheet. MEMO/15/5612. Brussels, 08.09.2015.

59 Europaratsberichterstatter Dick Marty, zit. in: Gössner, Rolf (2009): EU-Terrorliste. Feindstrafrecht auf europäisch. In: Blätter für deutsche und internationale Politik (3/2009), S. 13–16 (15).

60 Sullivan, Gavin / Hayes, Ben (2010): Blacklisted. Targeted sanctions, preemptive security and fundamental rights. Berlin: ECCHR, S. 43 ff.

fahrensrechte wie des Rechts, gehört zu werden, und des Grundsatzes des kontradiktorischen Verfahrens hinreichend zu garantieren, auf der anderen Seite zum Ausgleich zu bringen."[61]

Damit beschritt das oberste Gericht der EU einen ähnlichen Weg wie das Bundesverfassungsgericht. Karlsruhe hatte bereits 1999 entschieden, dass die verfassungsrechtliche Absicherung der Rechtsschutzgarantie nicht dadurch unterlaufen werden dürfe, dass einem Gerichtsverfahren Unterlagen vorenthalten werden, weil die Gefahr bestehe, dass Klagende im Rahmen des Akteneinsichtsrechts Kenntnis von geheimhaltungsbedürftigen Informationen erhielte: „Das Gericht muß die tatsächlichen Grundlagen selbst ermitteln und seine rechtliche Auffassung unabhängig von der Verwaltung, deren Entscheidung angegriffen ist, gewinnen und begründen".[62] Entsprechend schlug das Verfassungsgericht die Möglichkeit eines „in camera"-Verfahrens vor, um die „Belange der Geheimhaltung bestimmter Vorgänge und die Rechtsschutzansprüche des Betroffenen [...] dadurch besser in Einklang" zu bringen.[63]

Ausdrücklich in Kauf nimmt das Gericht damit den Verzicht auf ein kontradiktorisches Verfahren, in dem Betroffene sich zu den verhandelten Sachverhalten äußern und so auf das Verfahren und dessen Ergebnis Einfluss nehmen können. Der Anspruch auf rechtliches Gehör stehe in engem Zusammenhang mit der Rechtsschutzgarantie und könne daher eingeschränkt werden, „wenn dies durch sachliche Gründe hinreichend gerechtfertigt ist".[64] Da im Verwaltungsverfahren, anders als im Strafverfahren, „in dubio pro reo" nicht gelte, würde das „ungeschmälerte rechtliche Gehör [...] die Effektivität des Rechtsschutzes im Ergebnis herabsetzen, statt sie zu stützen".[65]

In der Folge wurde § 99 der Verwaltungsgerichtsordnung (VwGO) geändert und die Möglichkeit des „in camera"-Verfahrens in den deutschen Verwaltungsprozess eingeführt. Seither können Betroffene in Verfahren vor Verwaltungsgerichten beantragten, dass geprüft wird, ob die die Geheimhaltung von Unterlagen rechtmäßig ist. Damit wird ein Nebensacheverfahren vor einem besonderen Fachsenat des zuständigen Oberverwaltungsgerichts beziehungsweise des Bundesverwaltungsgerichts eröffnet, der zu entscheiden hat, ob die exekutive Weigerung, Informationen im Hauptsacheverfahren vorzulegen, rechtmäßig ist. Dabei gelten die Vorschriften des Geheimschutzes, das heißt das nichtrichterliche Personal muss sicherheitsüberprüft sein und gegebenenfalls sind Dokumente durch Mitglieder des Senats in besonderen Räumlichkeiten der obersten Aufsichtsbehörde einzusehen. Zudem dürfen die Entscheidungsgründe „Art und Inhalt" der überprüften Geheimunterlagen nicht erkennen lassen. Entscheidungen von „in camera"-Senaten der Oberverwaltungsgerichte sind vor dem Bundesverwaltungsgericht anfechtbar.[66]

Ausschlaggebend war die Verfassungsbeschwerde eines ehemaligen Beamten, dem im Rahmen der Sicherheitsüberprüfung aufgrund der Erklärungen von Gewährspersonen durch das Bayerische Landesamt für Verfassungsschutz ein „Charakterzug" attestiert wurde, „der dazu führen könne, daß er Opfer einer nachrichtendienstlichen Verstrickung werde".[67] Doch Anwendung finden „in camera"-Verfahren zum Beispiel auch in Streitfällen über Auskunftsrechte oder gefahrenabwehrrechtliche Verwaltungsentscheidungen, etwa wenn auf Grundlage von geheimen Informationen Ausreiseverbote oder aufenthaltsrechtliche Sanktionen gegen „ausländische Gefährder" verhängt werden. Die Herausforderung für Betroffene bleibt in jedem Fall, dass sich mit der Eröffnung eines Nebensacheverfahrens die Hürden für den Zugang zum Recht multiplizieren und bereits in der ersten Instanz leicht fünf Jahre oder mehr vergehen können, bis ein Urteil gesprochen wird.[68]

3.5 Wirksame Kontrolle?

Festzuhalten bleibt, dass im Bereich des Staats- und Verfassungsschutzes die Hürden für den Zugang zum Recht hoch sind. Auch wenn nachträgliche Benachrichtigungspflichten oder Auskunftsrechte Betroffener rechtlich garantiert sind, kann sich ihre Realisierung in der Praxis äußerst schwierig gestalten: Das Spektrum reicht von kleineren Hürden, wie dem Einfordern be-

61 Europäischer Gerichtshof (2013): Urteil vom 18.07.2013 (Kadi II), Aktenzeichen C–584/10 P, C–593/10 P und C–595/10 P, Rn. 125.
62 Bundesverfassungsgericht (1999): Beschluss vom 27.10.1999. 1 BvR 385/90. In: BVerfGE 101, 106 (Akteneinsichtsrecht), S. 123.
63 Ebda, S. 128.
64 Ebda,. S. 129.
65 Ebda., S. 130.
66 § 99 Abs. 2 VwGO.
67 BVerfGE 101, 106, S. 123.
68 Busch, Heiner / Furmaniak, Angela / Kauß, Udo (2015): Mühsam, aufwändig, aber wichtig. Kurzer Lehrgang über Auskünfte vom Verfassungsschutz. Interview mit Angela Furmaniak und Udo Kauß. In: Bürgerrechte & Polizei/CILIP (Heft 107), S. 29–41.

glaubigter Ausweiskopien, wenn Betroffene ein Auskunftsersuchen stellen, bis hin zur Überforderung der Behörden mit der Benachrichtigung Betroffener. Regelmäßig begrenzt ist der individuelle Zugang zum Recht dann, wenn mutmaßlich Sicherheits- und Geheimhaltungsinteressen überwiegen. Auch wenn diese Grenzen im nachrichtendienstlichen Bereich am offensichtlichsten sind, so sind auch verdeckte Maßnahmen des polizeilichen Staatssschutz gut gesichert gegen mögliche Anfechtungen durch Betroffene, zum Beispiel dann, wenn es um den Einsatz von Verdeckten Ermittlern geht.

Dort, wo der Rechtsweg ausgeschlossen ist und dieser Mangel geheilt werden soll durch Ersatzverfahren, wie die richterliche Kontrolle des Unterlassens der Benachrichtigung oder die Aufsicht durch Datenschutzbeauftragte oder parlamentarische Instanzen wie die G 10-Kommissionen und Kontrollgremien, ist die Frage zu stellen, ob diese Kontrolle den grund- und menschenrechtlichen Anforderungen genügt. Das heißt, sie muss materiell und verfahrensmäßig der gerichtlichen Kontrolle gleichwertig und mindestens ebenso wirkungsvoll sein, auch wenn Betroffene keine Mitwirkungsmöglichkeit haben.[69]

Bei der richterlichen Prüfung des Unterlassens der Benachrichtigung von durch verdeckte Maßnahmen Betroffenen fehlt - ebenso wie in anderen der hier beschriebenen Verfahren - das kontradiktorische Element. Die Betroffenen werden nicht gehört. Fraglich ist zudem, ob sie ebenso wirkungsvoll ist. Über die Praxis ist wenig bekannt. Nimmt man jedoch die Erkenntnisse zur Wirksamkeit des *ex ante* Richtervorbehalts bei verdeckten Maßnahmen als Indikator,[70] könnte man vermuten, dass auch bei *ex post* Prüfungen aus Gründen der Arbeitsökonomie nur eine relativ oberflächliche Prüfung der exekutiven Begründungen stattfindet. Allerdings fehlen solide und zudem aktuelle empirische Befunde. Ebenso wenig ist bekannt, welchen Einfluss der Verzicht auf das rechtliches Gehör von Betroffenen und das Geheimschutz-Korsett auf die Qualität der gerichtlichen Entscheidungen in den „in camera"-Verfahren haben.

Umstritten ist die Wirksamkeit der Kontrolle durch die gerichtsähnlichen **G 10-Kommissionen**, auf die an dieser Stelle nur für die Bundesebene eingegangen werden kann: Die vier vom Parlamentarischen Kontrollgremium des Deutschen Bundestages gewählten Mitglieder und ihre Stellvertreter arbeiten ehrenamtlich und erhalten lediglich eine Aufwandsentschädigung. Die Kommission trifft sich einmal im Monat, um ein wachsendes Aufgabenspektrum zu bearbeiten: Gemäß Artikel 10-Gesetz ist sie zuständig für die Prüfung der Post- und Telekommunikationsüberwachungsanordnungen der Nachrichtendienste des Bundes, die Kontrolle der gesamten Erhebung, Verarbeitung und Nutzung der durch entsprechende Maßnahmen erlangten personenbezogenen Daten sowie der Begründungen für den Verzicht auf nachträgliche Benachrichtigungen. Außerdem soll die Kommission Beschwerden von Menschen nachgehen, die glauben, dass sie überwacht werden. Hinzu kommt seit 2002 die Prüfung der Anordnung besonderer Auskunftsverlangen, mit denen die Nachrichtendienste des Bundes Informationen bei Fluggesellschaften, Geldinstituten sowie Telekommunikations- und Telemediendienstleistern abfragen können. Seit Anfang 2015 ist die Kommission außerdem zuständig für die Prüfung der eingangs genannten erweiterten Nutzung von Daten aus Antiterror- oder Rechtsextremismusdatei für Analyseprojekte durch Sicherheitsbehörden des Bundes. Entsprechend voll sind die Tagesordungen des Gremiums. Bereits 2011 sollen bis zu 70 Fälle in den vier bis fünf Stunden dauernden Sitzungen entschieden worden sein.[71]

Dass die Kommission angesichts dessen in der Lage ist, effektiven Rechtsschutz zu gewährleisten ist fragwürdig. Zumindest aus der Vergangenheit ist bekannt, dass die sie ihre Entscheidungen regelmäßig nur auf den Sachvortrag der Exekutive stützte und ihre eigentlich umfassenden Kontrollbefugnisse höchstens in Einzelfällen wahrgenommen hat.[72] Einzelne Mitglieder der Kommission betonen – ohne jedoch in die Details zu gehen – hingegen, dass es seit Ende der 1990er Jahre gelungen sei, die Kontrollfunktion effektiv auszubauen und zu nutzen.[73] Allerdings wurde durch die Arbeit des NSA-Untersuchungsausschusses deutlich, dass sich angesichts ihrer technischen Komplexität und der schieren Masse der Überwachungsziele – den sogenannten „Selektoren" – insbesondere die strategische

69 Bundesverfassungsgericht (1970): Urteil vom 15.12.1970. 2 BvF 1/69. In: BVerfGE 30, 1 (Abhörurteil), S. 23.

70 Eine Synopse der empirischen Befunde von Studien aus dem Jahr 2003 bei Gusy, Christoph (2015): Zukunft der Richtervorbehalte. In: Barton, Stephan / Kölbel, Ralf / Lindemann, Michael (Hg.): Wider die wildwüchsige Entwicklung des Ermittlungsverfahrens. Baden-Baden: Nomos, S. 196–217 (197 ff.).

71 Koch, Hannes (2011): G 10-Kommission – eine Frage des Glaubens. In: Der Freitag, 20. 10. 2011. https://www.freitag.de/autoren/der-freitag/eine-frage-des-glaubens (Stand: 20. 08. 2015).

72 Kornblum, Thorsten (2011): Rechtsschutz gegen geheimdienstliche Aktivitäten. Berlin: Duncker & Humblot, S. 194 f.

73 Huber, Bertold (2014): Die Fernmeldeaufklärung des Bundesnachrichtendienstes. Rechtsgrundlagen und bestehende Regelungsdefizite. In: vorgänge (Heft 206/207), S. 42–49 (46 f.).

Fernmeldeüberwachung des Bundesnachrichtendienstes einer wirksamen Kontrolle entzieht, wie inzwischen selbst Mitglieder der Kommission einräumen.[74]

Die Aufsicht durch die **Datenschutzbeauftragen** ist bereits in rechtlicher Hinsicht mehrfach beschränkt. Wird zum Beispiel, wie bereits erwähnt, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) von Betroffenen eingeschaltet, um gemäß § 19 Abs. 6 Bundesdatenschutzgesetz (BDSG) beziehungsweise § 15 Abs. 4 Bundesverfassungsschutzgesetz (BVerfSchG) stellvertretend Auskunftsrechte gegenüber Behörden des Bundes wahrzunehmen, so kann das zuständige Ministerium als oberste Bundesbehörde das Auskunftsverlangen der Aufsichtsinstanz ablehnen, wenn es „im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde". Diese formelle Beschränkung von Auskunftsverlangen entspricht der „Staatswohlklausel" in § 24 Abs. 4 BDSG, mit der die datenschutzrechtliche Kontrolle durch die BfDI insofern eingeschränkt ist, als ihre grundsätzlichen Informations- und Inspektionsrechte im Einzelfall suspendiert werden können, wenn die Auskunft oder Einsicht in Unterlagen nach Feststellung der obersten Bundesbehörde die nationale Sicherheit gefährden würde. Zusätzlich ist die Aufsicht dann problematisch, wenn die Rechtmäßigkeit der Verarbeitung personenbezogener Daten mit Informationen begründet wird, die durch nachrichtendienstliche Kommunikationsüberwachung erlangt wurden. Gemäß § 24 Abs. 2 BDSG sind eben jene Daten, die der Kontrolle durch die G 10-Kommission unterliegen, ausdrücklich von der Kontrolle durch die BfDI ausgenommen, es sei denn die Kommission erbittet ausdrücklich Unterstützung. Andererseits ist die G 10-Kommission nur zur Kontrolle von G 10-Daten befugt, jedoch nicht von Daten, deren Speicherung mit Informationen aus einer G 10-Überwachung begründet wird. Deutlich wurde diese Kontrolllücke, die sich aus dem Nebeneinander der Aufsichtsgremien ergibt, insbesondere bei der Antiterrordatei. Entsprechend sah sich das Bundesverfassungsgericht veranlasst, den Gesetzgeber daran zu erinnern, dass „auch die kontrollierende Kooperation zugunsten des Datenschutzes" zu ermöglichen ist.[75] Entgegen der Mahnung aus Karlsruhe wurde eine entsprechende Reform bei der Novellierung des Antiterrordateigesetzes versäumt. Stattdessen muss sich die BfDI nunmehr mit dem informellen Zugeständnis des Bundesministerium des Innern begnügen, dass sie zur Erfüllung ihrer Aufgaben auch G 10-Daten prüfen darf.[76]

Zu den formellen Mängeln der Beaufsichtigung der Sicherheitsbehörden durch die Datenschutzbeauftragten kommen die praktischen Probleme, die sich aus den knappen Ressourcen ergeben. Das für die Kontrolle der Polizeien und Nachrichtendienste des Bundes zuständige Referat V der BfDI operiert beispielsweise mit nicht einmal zehn Personalstellen.[77] Vor diesem Hintergrund richtete die Bundesbeauftragte in ihrem Tätigkeitsbericht 2013/2014 einen dramatischen Appell an den Bundestag und erklärte vor dem Hintergrund der massiven Aufrüstung der Sicherheitsbehörden seit 2001:

„Auf Seiten der Kontrollorgane ist keine entsprechende Entwicklung erfolgt, das heißt auch insoweit bestehen gravierende gesetzgeberische Defizite, die im Interesse der Bürgerinnen und Bürger schnellstmöglich beseitigt werden müssen. In Folge dieser Entwicklung ist es mir angesichts der mir zur Verfügung stehenden geringfügigen Personal- und Sachmittel nicht mehr möglich, meine gesetzlich zugewiesenen Beratungs- und Kontrollaufgaben angemessen zu erfüllen. Damit ist es mir auch nicht mehr möglich, die vom Bundesverfassungsgericht in seinem Urteil zum Antiterrordateigesetz betonte Kompensationsfunktion meiner Kontrollen für die betroffenen Bürgerinnen und Bürger sachgerecht zu gewährleisten, d. h. an Stelle der Betroffenen zu überprüfen, ob ihre Rechte bei heimlichen Eingriffen der Sicherheitsbehörden gewahrt worden sind."[78]

Anders als G 10-Kommissionen und Datenschutzbeauftragte ist den **Parlamentarischen Kontrollgremien** nicht explizit die Funktion des außergerichtlichen Rechtsschutzes zugewiesen. Für das Kontrollgremium des Deutschen Bundestages heißt es lediglich, dass die Bundesregierung hinsichtlich der Tätigkeiten ihrer Nachrichtendienste seiner Kontrolle unterliegt.[79] Dabei prüft es jedoch nicht nur die Zweckmäßigkeit, sondern auch die Rechtmäßigkeit nachrichtendienst-

74 Mascolo, Georg (2015): Wie ein deutscher Geheimdienst die ganze Welt abhört, in: Süddeutsche Zeitung, 22.04.2015. http://www.sueddeutsche.de/politik/spionage-mehr-als-ueberwacht-1.2447460 (Stand: 15.08.2015).
75 Bundesverfassungsgericht (2013): Urteil vom 24.04.2013 (Antiterrordateigesetz), 1 BvR 1215/07, Rn. 216.
76 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2015): Tätigkeitsbericht 2013 und 2014–25. Tätigkeitsbericht. Bonn, S. 36.
77 Stand September 2014 nach Auskunft der zuständigen Referatsleitung.
78 Ebda.
79 § 1 Abs. 1 Kontrollgremiumgesetz (PKGrG).

lichen Handelns.[80] Insofern könnte dem Kontrollgremium hinsichtlich des Einsatzes nachrichtendienstlicher Mittel eine Rechtsschutzfunktion zukommen, als dass es von den Diensten gemäß § 9 Abs. 3 BVerfSchG über bestimmte grundrechtsintensive Einzelmaßnahmen zu informieren ist und gegebenenfalls die Legalität derselben hinterfragen könnte.[81] Jenseits dessen soll das Kontrollgremium allerdings nur über die Dienstvorschriften zum Einsatz nachrichtendienstlicher Mittel informiert werden sowie über die „allgemeine Tätigkeit" und „Vorgänge von besonderer Bedeutung".[82] Zwar kann das Kontrollgremium auch detailliertere Informationen zu „sonstigen Vorgängen" verlangen sowie Einsicht in Akten und Dateien, Zutritt zu Dienststellen und Befragung von Behörden- und Regierungsarbeiten.

Hierzu muss es aber wissen, wo Probleme virulent sein könnten und wonach zu fragen und zu suchen wäre. Angesichts der Informationshoheit der Exekutive dürfte eben dies aber ein zentrales Problem sein. Selbstbescheiden heißt es im Tätigkeitsbericht 2012/2013, dass die Informationspolitik von Bundesregierung und Nachrichtendiensten „soweit dies für das Gremium ersichtlich war" meist angemessen war.[83] Ein weiteres Hindernis für eine wirksame Aufsicht des Gremiums sind seine knappen Ressourcen: In der 18. Legislaturperiode sind neun viel beschäftigte Bundestagsabgeordnete seine Mitglieder. Unterstützt werden sie zum einen von sechs sicherheitsüberprüften Fraktionsmitarbeitenden, die nach § 11 PKGr befugt sind, die vom Gremium beigezogenen Akten und Dateien einzusehen und die Beratungsgegenstände des Gremiums mit seinen Mitgliedern zu erörtern, in der Regel aber nicht an dessen Sitzungen teilnehmen dürfen, und zum anderen von einem Sekretariat der Bundestagsverwaltung mit mittlerweile 13 Stellen.[84] Das Sekretariat unterstützt zwar auch die Arbeit der G 10-Kommission und des Zollfahndungsdienstgesetz-Gremiums, sein Personal wurde allerdings insbesondere als Konsequenz aus den Ergebnissen des NSU-Untersuchungsausschusses durch die Schaffung eines siebenköpfigen „operativen Stabs" (auch „Task Force" genannt) seit Sommer 2014 deutlich aufgestockt.[85] Unter dem Strich liegt die Verantwortung für die Kontrolle des rechtmäßigen Handelns der etwa 10.500 Mitarbeitenden der Nachrichtendienste des Bundes somit in den Händen von knapp 30 Personen, die im Jahr 2015 über ein Sachmittelbudget von 100.000 Euro verfügten.[86] Selbst wenn durch den neuen „operativen Stab" die Möglichkeit geschaffen wurde, die *de jure* existierenden Kontrollrechte, anders als in der Vergangenheit, auch tatsächlich wahrzunehmen, ist kaum zu erwarten, dass auf diese Weise die Rechtsmäßigkeit individueller Maßnahmen stellvertretend für Betroffene effektiv kontrolliert werden kann.

Hinzu kommt das Problem, dass die Aufsichtsrechte des Kontrollgremiums begrenzt sind: Zum einen ist die Bundesregierung nur zur Auskunft über Informationen und Gegenstände verpflichtet, die der Verfügungsberechtigung der Nachrichtendienste des Bundes unterliegen.[87] Eine solche Verfügungsberechtigung bestehe in der Regel nicht, „wenn es sich um Informationen handelt, die von ausländischen Behörden übermittelt worden sind", so der Hinweis der Begründung des Kontrollgremiumgesetzes von 1999[88] auf die „Third Party Rule"[89] des internationalen Geheimdienstgeschäfts. Denkbar sind aber auch Bund-Länder-Konkurrenzen. In solchen Fällen bedürfe des der Abstimmung zwischen Kontrollgremien, „um etwaige Kontrolllücken zu vermeiden".[90] Zum anderen kann die Bundesregierung aus „zwingenden Gründen des Nachrichtenzugangs", „aus Gründen des Schutzes von Persönlichkeitsrech-

80 Deutscher Bundestag (2013): Bericht über die Kontrolltätigkeit gemäß § 13 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Berichtszeitraum November 2011 bis Oktober 2013). Unterrichtung durch das Parlamentarische Kontrollgremium. Drucksache 18/217, 19. 12. 2013, S. 3.

81 Für Bundesnachrichtendienst und Militärischen Abschirmdienst verweisen § 3 BNDG und § 5 MADG auf § 9 BVerfSchG.

82 § 4 Abs. 1 PKGrG.

83 Deutscher Bundestag (2013): Bericht über die Kontrolltätigkeit gemäß § 13 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Berichtszeitraum November 2011 bis Oktober 2013). Unterrichtung durch das Parlamentarische Kontrollgremium. Drucksache 18/217, 19. 12. 2013, S. 3.

84 Die Zahlenangaben basieren auf einer schriftlichen Mitteilung des damaligen PKGr-Vorsitzenden MdB Clemens Binninger vom 17. 09. 2014.

85 dpa (2014): Mehr Kontrolle für den Bundestag. Taskforce soll Geheimdienste überwachen. In: Handelsblatt, 01. 07. 2014. http://www.handelsblatt.com/politik/deutschland/mehr-kontrolle-fuer-den-bundestag-taskforce-soll-geheimdienste-ueberwachen/10136656.html (Stand: 22. 08. 2015).

86 Bundeshaushaltsgesetz 2015, Einzelplan 02, Titel 526 05–011.

87 § 6 Abs. 1 PKGrG.

88 Deutscher Bundestag (1999): Entwurf eines Gesetzes zur Änderung von Vorschriften über parlamentarische Gremien. Drucksache 14/539, 16.09.1999, S. 7.

89 Die „Third Party Rule" meint, dass Informationen, die ein Dienst an einem Partnerdienst liefert, im „Besitz" des übermittelnden Dienstes bleiben und an eine dritte Partei – eben auch Aufsichtsinstanzen – nur mit dessen Einverständnis weitergegeben werden dürfen.

90 Deutscher Bundestag (1999): Entwurf eines Gesetzes zur Änderung von Vorschriften über parlamentarische Gremien. Gesetzentwurf der Fraktionen SPD, CDU/CSU, Bündnis 90/Die Grünen, FDP. Drucksache 14/539, 16. 03. 1999, S. 7.

ten Dritter" oder „wenn der Kernbereich der exekutiven Eigenverantwortung betroffen ist" die Auskunft verweigern.[91]

4 Zusammenfassung

Das Menschenrecht auf wirksame Beschwerde gilt auch in der Terrorismus- und Extremismusbekämpfung. Auch in diesem Feld ist der Zugang zum Recht zu gewährleisten. Ist Betroffenen die unmittelbare Überprüfung polizeilicher oder nachrichtendienstlicher Maßnahmen durch Gerichte aufgrund ihres heimlichen Charakters versagt, so muss der Gesetzgeber die Behörden zur nachträglichen Benachrichtigung verpflichten, damit Betroffenen der Rechtsweg offen steht. Wird auch diese Möglichkeit aus legitimen Sicherheits- und Geheimhaltungsinteressen dauerhaft verstellt, so müssen gleichwertige Ersatzverfahren etabliert werden, die den Ausschluss vom Rechtsweg kompensieren. Hierzu muss die Kontrolle unabhängig und stetig sein und Zugang zu allen relevanten Informationen haben, damit eine selbständige Aufklärung des Sachverhalts möglich ist.

Gemessen an diesen Vorgaben ist die Entwicklung in Deutschland widersprüchlich: Einerseits hat der Gesetzgeber in den vergangenen drei Jahrzehnten insbesondere aufgrund der Rechtsprechung des Bundesverfassungsgerichts sukzessive die Voraussetzungen für wirksame Beschwerden gegen mutmaßlich rechtswidriges Handeln von Sicherheitsbehörden verbessert: Auskunftsrechte wurden gestärkt und Benachrichtigungs- und Mitteilungspflichten erweitert; die Möglichkeit des „in camera"-Verfahrens wurde geschaffen, um der Verwaltungsgerichtsbarkeit auch die Prüfung geheimer Informationen zu ermöglichen. Gestärkt wurden auch die Unabhängigkeit und Kompetenzen der Instanzen außergerichtlicher Kontrolle. Andererseits wurde der Apparat und die Befugnisse der Sicherheitsbehörden in einem Maße ausgebaut, mit dem die Rechtsschutzinstrumente nicht Schritt halten. Gegenüber der Dynamik technologischer Innovation sowie dem Machtzuwachs und der Entgrenzung von polizeilichem Staatsschutz und Nachrichtendiensten wirken die Betroffenenrechte bescheiden und stagnieren die Ressourcen der Kontrollinstanzen.

Im Ergebnis bestehen nicht nur deutliche rechtliche Schutzlücken, sondern auch erhebliche praktische Herausforderungen, wenn es um den effektiven Zugang zum Recht im Feld der Terrorismus- und Extremismusbekämpfung geht. Diese Diagnose gilt – wenngleich mit signifikanten Unterschieden – bereichsübergreifend für polizeiliche Gefahrenabwehr, Strafverfolgung und die Aufklärung durch die Nachrichtendienste. Für all jene heimlichen strafprozessualen Maßnahmen, die bereits verrechtlicht sind, sind regelmäßig Instrumente des präventiven sowie nachträglichen Rechtsschutzes durch Richtervorbehalte und Benachrichtigungspflichten gesetzlich vorgesehen. Hingegen unterliegt deren Ausgestaltung im polizeirechtlichen Bereich teilweise erheblichen verfassungsrechtlichen Bedenken. Im nachrichtendienstlichen Bereich ist eine Benachrichtigung Betroffener größtenteils gar nicht oder nur unzureichend normiert. Grundsätzlich problematisch bleibt der Einsatz menschlicher Quellen, da Betroffene aufgrund der Kollision ihrer Rechte mit denen der zu schützenden V-Leute oder Verdeckten Ermittler auch dann das Nachsehen haben, wenn der Zweck der Überwachung durch eine Benachrichtigung nicht länger gefährdet wäre. Auch die Kontrolle neuer technischer Mittel ist jeweils solange problematisch, bis die rechtlichen Grauzonen der Innovation durchreguliert sind.

Empirische Untersuchungen deuten auf die Schwierigkeiten hin, die mitunter aufwändigen Benachrichtigungspflichten in der behördlichen Praxis adäquat umzusetzen. Die Wahrnehmung von Auskunftsrechten stößt insbesondere dort an Grenzen, wo ein Informationsaustausch im Rahmen behörden- oder grenzübergreifender Sicherheitskooperation tangiert ist oder selbst der Datenschutzaufsicht aus Gründen der nationalen Sicherheit eine Auskunft verweigert werden kann. Somit gibt es ein weites Feld sicherheitsbehördlichen Handelns, das der Kenntnisnahme Betroffener und damit auch einer möglichen gerichtlichen Überprüfung entzogen ist. Diese dunklen Ecken des Rechtsstaates auszuleuchten und ersatzweise Rechtsschutz zu gewährleisten, wäre die Aufgabe der verschiedenen Aufsichtsgremien. Dass sie angesichts der rechtlichen Kontrolllücken und der unübersehbaren Asymmetrie der Ressourcen in der Lage sind, diese Aufgabe wirkungsvoll wahrzunehmen, wird jedoch auch von ihnen selbst bezweifelt. Damit ist freilich nichts gesagt darüber, ob und in welchem Ausmaß rechtswidriges Handeln deutscher Sicherheitsbehörden zu beanstanden ist. Doch wenn Betroffene mangels Rechtsschutzmöglichkeiten diesem Handeln ohnmächtig gegenüberstehen und auch die Ersatzverfahren zum

91 § 6 Abs. 2 PKGrG

Schutz vor behördlicher Willkür nur begrenzt wirksam sind, dann ist, wie das Bundesverfassungsgericht 1970 warnte, die Menschenwürde angetastet.

5 Empfehlungen

Angesichts der aufgezeigten Schutzlücken besteht dringender Bedarf zur Stärkung des Rechtsschutzes gegenüber heimlichen Maßnahmen der Terrorismus- und Extremismusbekämpfung. Auch wenn derzeit vor allem die Kontrolle der Nachrichtendienste diskutiert wird, muss dabei auch der polizeiliche Staatsschutz in den Blick genommen werden.

Die Rechte Betroffener, über heimliche Maßnahmen und die Verarbeitung personenbezogener Daten informiert zu werden, stärken

Der Gesetzgeber auf Bundes- und Landesebene sollte flächendeckend Benachrichtigungspflichten einführen. Ausnahmen davon muss er eng und präzise fassen und verfahrenssicher regeln. Der Gesetzgeber und die Exekutive müssen die Rechtspraxis beobachten, damit gegebenenfalls durch Schulungen oder Anpassungen von Verwaltungsroutinen nachgesteuert werden kann. Sowohl die Sicherheits- als auch die Datenschutzbehörden sollten zur Wahrnehmung von Auskunftsrechten ermutigen und praktische Hürden minimieren. Zudem sollte der Gesetzgeber in Bund und Ländern das Recht auf Auskunft mit folgender Stoßrichtung reformieren: Müssen Daten gegenüber Betroffenen wirklich geheim gehalten werden, sollten Behörden die nicht geheimhaltungsbedürftigen Umstände mitteilen und die geheimhaltungsbedürftigen Umstände so umschreiben, dass die Auskunft so detailliert wie möglich ausfällt, ohne das Geheimnis zu verraten. Verweigern Sicherheitsbehörden in bestimmten Bereichen generell die Auskunft, sollte dies proaktiv an die zuständigen Datenschutzbeauftragten gemeldet werden, damit diese überprüfen können, ob tatsächlich ein grundsätzlicher Ausnahmetatbestand vorliegt.[92]

Befugnisse und Mittel der Aufsichtsgremien stärken

Der Gesetzgeber muss die „Staatswohlklauseln" im Datenschutzrecht von Bund und Ländern beseitigen, aufgrund derer selbst sicherheitsüberprüften Mitarbeitenden von Datenschutzbehörden die Einsicht in Unterlagen und Inspektionen aus Gründen nationaler Sicherheit in Einzelfällen versagt werden kann. Auch sollte er Kontrolllücken, die aus der Fragmentierung der Kontrolle resultieren, gesetzgeberisch schließen: Eine Prüfung von G 10-Daten zu Zwecken der Datenschutzaufsicht ist nicht nur informell zu gewährleisten. Vertieft werden sollten auch Reformüberlegungen, wie Bund-Länder-Konkurrenzen bei der Aufsicht gegenüber einer zunehmend vernetzten Sicherheitsarchitektur minimiert werden können.[93] Gleiches gilt für die Frage, wie ein wirksames Regime zur multilateralen Kontrolle internationaler Sicherheitskooperation etabliert werden kann. Dabei sollte es neben dem Austausch von Erfahrungen und „best practices", wie er bereits beispielsweise bei der europäischen Konferenz der parlamentarischen Kontrollgremien oder der International Intelligence Review Conference stattfindet, mindestens auch um die Möglichkeit gehen, strukturelle Bedingungen der Sicherheitskooperation zum Beispiel in Form von internationalen Geheimdienstabkommen, parlamentarisch zu überprüfen.[94] Selbstverständlich müssen erweiterte Kontrollrechte auch wirksam wahrgenommen werden können. Hierzu sollten die Parlamente nicht nur die Personal- und Sachmittel der Aufsichtsgremien deutlich aufzustocken, sondern auch eine Professionalisierung der bislang ehrenamtlich arbeitenden G 10-Kommissionen anstreben. Was die Rolle richterlicher Prüfung betrifft, sollten Studien zur Wirksamkeit des Richtervorbehalts aktualisiert und um die Kontrolle unterlassener Benachrichtigungen erweitert werden, damit gegegebenfalls Änderungen der Praxis angeregt werden können. Hinsichtlich der Überlegungen zu weitergehenden Reformen ist anzumerken, dass auch die parlamentarische Aufsicht Rechtsschutzfunktionen hat und somit möglichst frei

92 Die Vorschläge zur Stärkung der Auskunftsrechte orientieren sich an den Empfehlungen von Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen (2001): Modernisierung des Datenschutzrechtes. Gutachten im Auftrag des Bundesministeriums des Innern. Berlin: Bundesministerium des Innern, S. 170 ff.

93 Verwiesen sei hier beispielsweise auf die Überlegungen des NSU-Untersuchungsausschusses des Deutschen Bundestages, die Befragungsrechte des Parlamentarischen Kontrollegremiums des Deutschen Bundestages auszuweiten auf Personen, die nicht für die Nachrichtendienste des Bundes arbeiten, sondern etwa für Landesverfassungsschutzämter tätig sind. Deutscher Bundestag (2013): Beschlussempfehlung und Bericht des 2. Untersuchungsausschusses nach Artikel 44 des Grundgesetzes. Drucksache 17/14 600, 22. 08. 2013, S. 865.

94 van Ginkel, Bibi (2012): Towards the intelligent use of intelligence: Quis Custodiet ipsos Custodes? ICCT Research Paper. The Hague: International Centre for Counter-Terrorism.
http://www.icct.nl/download/file/ICCT-van-Ginkel-Intelligent-Use-of-Intelligence-August-2012.pdf (PDF, 354 KB, Stand: 19. 08. 2015).

von parteipolitischen Opportunitäten sein sollte. Angesichts dessen scheint die Idee eines unabhängigen, vom Parlament beauftragten Beauftragten zur Kontrolle der Dienste plausibel. Statt jedoch die weitere Fragmentierung der Kontrolle durch die Einrichtung eines neuen Gremiums voranzutreiben, sollte überlegt werden, wie sich existierende Strukturen wie zum Beispiel die Datenschutzbeauftragte entsprechend ausbauen lassen.

Instrumente schaffen, die das Handeln von Sicherheitsbehörden transparenter machen

Bei allen Bemühungen um eine Stärkung der Rechtsschutzes durch den Ausbau der Kontrolle darf jedoch nicht übersehen werden, dass dieser angesichts des Kräfteungleichgewichts immer praktische Grenzen gesetzt sein werden, es sei denn, man wollte einen „Dienst neben dem Dienst" aufbauen, was die bestehenden Probleme der Rechenschaftslegung potenzieren würde.[95] Deshalb sollte der Gesetzgeber in Bund und Ländern Instrumente schaffen, die das Handeln von Sicherheitsbehörden transparenter machen: Zu denken ist, erstens, an einen Ausbau von Pflichten, den Parlamenten und der Öffentlichkeit über den Umfang des Einsatzes heimlicher Maßnahmen zu berichten. Zweitens müssen Informationsfreiheitsrechte erweitert werden. Hierzu sollten alle Bundesländer und der Bund Informationsfreiheitsgesetze schaffen, die Nachrichtendienste nicht *per se* von Fragerechten ausnehmen, sondern diese stattdessen verpflichten die Geheimhaltungsbedürftigkeit von Informationen im Einzelfall zu begründen. Drittens sollte der Schutz von „Whistleblowern", die auf Rechtsverletzungen und Missstände aufmerksam machen, gestärkt werden. Dass dies nur dann Sinn macht, wenn gleichzeitig jene vor Repression geschützt sind, die Hinweise von „Whistleblower" öffentlich machen, liegt auf der Hand.

Sicherheitsgesetze menschen- und grundrechtsbasiert evaluieren

Doch selbst bei der Gewährleistung des Menschenrechts auf wirksame Beschwerde, bleiben andere Menschenrechte im Recht im Feld der Terrorismus- und Extremismusbekämpfung verletzlich. Selbst wenn der Zugang zum Recht in diesem Feld umfänglich eröffnet wäre, entbindet dies den Staat nicht von seiner grundsätzlichen Pflicht zur Achtung der Menschenrechte. Angesichts der Ungewissheiten über die tatsächlichen Folgen weitreicher Eingriffsbefugnisse von Sicherheitsbehörden und über die heilende – sprich: die Verhältnismäßigkeit garantierende – Wirkung, der hier vorgeschlagenen Maßnahmen, sollte der Gesetzgeber Sicherheitsgesetze grundsätzlich menschen- und grundrechtsbasiert evaluieren.[96]

95 Pütter, Norbert (2014): Geheimdienste besser kontrollieren? Zwischen Illusion und bewusster Täuschung. In: Bürgerrechte & Polizei/CILIP (Heft 105), S. 17–26 (25).

96 Weinzierl, Ruth (2006): Die Evaluierung von Sicherheitsgesetzen. Anregungen aus menschenrechtlicher Perspektive: Deutsches Institut für Menschenrechte. Berlin (Policy Paper Nr. 6).

Deutsches Institut für Menschenrechte

Zimmerstr. 26/27

10969 Berlin

Tel.: +49 (0)30 25 93 59 – 0

Fax: +49 (0)30 25 93 59 – 59

info@institut-fuer-menschenrechte.de

www.institut-fuer-menschenrechte.de